Security And Emergency Operations

Executive Budget Summary

Mission

Provide a domestic safeguards and security program for protection of nuclear weapons, nuclear materials, nuclear facilities, and classified and unclassified information, including cyber systems, against theft, sabotage, espionage, terrorist activities, or any loss or unauthorized disclosure that could endanger our National Security or disrupt operations. Provide an emergency operations program that ensures an integrated response to all Department of Energy emergencies to include capabilities (assets) to respond to any nuclear weapon accident or an act of nuclear terrorism within the United States or abroad. Provide a Critical Infrastructure Protection program to ensure the viability of the energy sector infrastructure nationwide. Provide a classification and declassification program that protects classified data, while ensuring availability of data to the public.

Strategy

To carry out this mission, the Department has established the Office of Security and Emergency Operations. This Office is working with the Secretary of Energy to implement a comprehensive plan that gives DOE the tools and authority to correct institutional problems and protect America's nuclear secrets. The program's coverage is comprehensive and includes cyber security; foreign visits and assignments; physical security; plutonium, uranium, and special materials inventory; and critical infrastructure protection.

The cyber security program will provide the policy and planning, training, technical development, and operations to provide consistent principles and requirements that line management can implement for the protection of classified and unclassified information. The foreign visits and assignment program will provide a central accounting center to track and analyze the details of all foreign visits and assignments for all DOE facilities to ensure that these are conducted in a secure manner. The plutonium, uranium, and special materials inventory program will maintain real-time, reliable, and complete information on DOE nuclear materials that are subject to special control and accounting procedures. Physical security will provide emphasis on nuclear, biological, and chemical weapons protection and detection equipment, and training. The critical infrastructure protection program will ensure that we support Presidential Decision Directive 63 and the mandates of the Critical Infrastructure Protection directive.

To further strengthen security DOE-wide, the Department may submit an Amendment to the FY 2001 Congressional request. The FY 2001 amendment would consolidate DOE safeguards and security expenditures within the Office of Security and Emergency Operations and allow enhanced allocation, tracking and monitoring of security costs Department-wide.

Major Changes

As a result of the DOE wide security reform announced on May 11. 1999, several Departmental functions were transferred to the Office of Security and Emergency Operations (SO). Beginning in FY 2000 funding for these programs will be budgeted for in the new Office of Security and Emergency Operations budget request. The programs transferred include: the Nuclear Safeguards and Security (NSS) program, the Security Investigations (SI) program and the Emergency Management (EM) program. The cyber security program was reorganized by combining the classified and unclassified computer security programs within the Office of the Chief Information Officer and is now included as part of the NSS program. In addition, the responsibility for the Nuclear Materials Management and Safeguards Systems was transferred from the Office of Nonproliferation and National Security to SO's Office of Plutonium, Uranium, and Special Material Inventory and now is part of the NSS program. The Office of Emergency Response, now part of the Emergency Management program, was transferred to SO from Defense Programs.

In late FY 1999, the Department created two new offices as part of the Secretary's security reform initiatives -- the Office of Plutonium, Uranium and Special Materials Inventory and the Office of Foreign Visits and Assignments. Both organizations are responsible for implementing important elements of the NSS program. The Office of Plutonium, Uranium and Special Materials Inventory serves as the single DOE organization for accurate tracking and accounting of all strategic nuclear materials, with a primary focus on separated plutonium, highly-enriched uranium, and other fissile materials. The Office of Foreign Visits and Assignments (FV&A) responds to PDD 61 requirements and increased Congressional attention which call for improved management of visits and assignments by foreign nationals to DOE sites nation-wide. The Office is also responsible for developing responsible program policies; collecting information concerning the number of foreign nationals visiting or assigned to DOE sites and the countries and the technologies involved; performing analytical studies on foreign visits and assignments; overseeing program implementation; representing the DOE in related internal and external forums; and improving critical program, technical, and automated information capabilities to collect and analyze data, (e.g., the Foreign Access Records Management System) to maintain and provide reliable information to the Secretary and the Congress.

There are also changes in the SI program pursuant to the National Defense Authorization Act for FY 2000. Section 3144 of the Act requires FBI rather then OPM background investigations of personnel in certain positions that have access to critical U.S. national security information.

Funding by Site

(dollars in thousands, whole FTEs)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Albuquerque Operations Office	64,313	59,716	64,509	4,793	8.0%
Chicago Operations Office	7,797	8,413	10,342	1,929	22.9%
Idaho Operations Office	1,637	2,008	2,409	401	20.0%
Nevada Operations Office	36,298	36,434	36,434	0	0.0%
Oak Ridge Operations Office	23,027	23,737	22,782	-955	-4.0%
Oakland Operations Office	23,021	27,451	27,315	-136	-0.5%
Ohio Field Office	0	100	100	0	0.0%
Pittsburgh Naval Reactors Office	1,850	1,234	1,145	-89	-7.2%
Richland Operations Office	4,080	6,494	6,262	-232	-3.6%
Savannah River Operations Office	2,802	4,410	4,763	353	8.0%
Schenectady Naval Reactors Office	550	461	461	0	0.0%
Washington Headquarters	110,213	127,279[a]	163,854	36,575	28.7%
Undistributed general reduction		-5,586[b]		5,586	100.0%
Sub-total Office of Security and Emergency Operations	275,588	292,151	340,376	48,225	16.5%
Less Use of Prior Year Balances	-1,821				0.0%
Less Offsets from Program Offices	-28,145	-20,000	-20,000	0	0.0%
Less Use of Proposed Supplemental	0	-8,000	0	+8,000	100.0%
Total Office of Security and Emergency Operations	245,662	264,151	320,376	56,225	21.3%
FTEs					
Chicago Operations Office	56	56	58	2	3.6%
Nevada Operations Office	5	5	2	-3	-60%
Headquarters	324	340	380	40	11.8%
Total FTEs	385	401	440	39	9.7%

[a]Includes use of $8 million supplemental.

[b]The amount of this general reduction associated with Emergency Response is under review within the Department.

Emergency Management

Program Mission

The Office of Emergency Operations (SO-40) consist of the Office of Emergency Management (SO-41) and the Office of Emergency Response (SO-42). The Office of Emergency Management serves as the point of contact and control for all Departmental emergency management activities and ensures an integrated response to emergencies affecting Departmental operations and activities or requiring Departmental assistance. The principal mission of the Office is to provide comprehensive, integrated emergency planning, preparedness, and response programs throughout the Department and to provide support to the Department's Headquarter and field operations. The Office responds to emergencies, issues all policy and guidance for the Department's emergency programs, and operates the HAZMAT Spill Center.

The Office of Emergency Response mission is to ensure that capabilities are in place to provide an appropriate response to any Department of Energy facility emergency and to any nuclear or radiological emergency within the United States or abroad. This is accomplished through the seven unique Departmental assets for both crisis and consequence management events described below:

The Aerial Measurement System detects, measures and tracks radioactive material at an emergency scene to determine contamination levels. The Atmospheric Release Advisory Capability develops predictive plots generated by sophisticated computer models. The Accident Response Group is deployed to manage or support the successful resolution of a U.S. nuclear weapons accident anywhere in the world. The Federal Radiological Monitoring and Assessment Center coordinates Federal radiological monitoring and assessment activities with those of state and local agencies. The Nuclear Emergency Search Team provides the nation’s specialized technical expertise to the Federal response in resolving nuclear/radiological terrorist incidents. The Radiological Assistance Program is usually the first responder for assessing the emergency situation and deciding what future steps should be taken to minimize the hazards of a radiological emergency. The Radiological Emergency Assistance Center/Training Site provides treatment and medical consultation for injuries resulting from radiation exposure and contamination, as well as serving as a training facility.

Additionally the Office of Emergency Response is charged through Presidential Decision Directive 39, the Atomic Energy Act, as amended, and Executive Order 12656, to ensure that the U.S. Government is prepared to provide technical and operational assistance in the resolution of a nuclear terrorist crisis within the U.S. or abroad. The Office also operates the Headquarters Emergency Operations Center, Communications Center and the Department's emergency communications network.

Program Goal

Support the National Security of the United States and prepare to combat terrorist by ensuring an integrated Departmental response to all emergencies, and maintaining the capability to respond to any nuclear weapons or radiological emergency in the United States or abroad. In addition, ensure that the appropriate infrastructure is in place to provide command, control, communications, and trained response personnel necessary to ensure the successful resolution of the emergency event.

Program Objectives

- Maintain national security and ensure protection of workers, the public, and the environment.
- Execute an integrated Departmental program in support of other U.S. Government agencies for combating terrorism and supporting crisis and consequence management to any terrorist act.
- Provide DOE's technical operational capability for worldwide response to a nuclear or radiological accident involving a nuclear weapon in either DOE or DOD custody.
- Continue ongoing efforts to improve response readiness to nuclear weapons of mass destruction posed by a terrorist threat contingency.
- Maintain capability to participate in interagency responses to emergencies in support of the Federal Response Plan, the National Contingency Plan, and the Federal Radiological Emergency Response Plan.
- Maintain the capability to provide technical advice and assistance to Departmental elements for cost effective implementation of the Emergency Operations programs.
- Develop, maintain, and promulgate policy, planning and preparedness guidance; and readiness assurance activities.
- Develop, maintain, and improve capabilities to detect and assess hazardous levels and characterization of radiation
- Operate and maintain the Headquarters Emergency Operations Center, Communications Center and the Department’s emergency communications network.
- Provide program management for operations of the HAZMAT Spill Center.

- Promote the Department's emergency policy interests in international fora.

- Support deployment and operational capabilities of nuclear and chemical dispersal models for emergency planning, preparedness and response to situations involving Departmental operations and activities.

- Ensure that National Laboratories' technically integrated (TI) projects promote advancements in training, drills and exercises. Through these TI advancements existing technical capabilities are improved or new leading edge technical capabilities are integrated in the ability to perform: Search, Access, Device Assessment, Diagnostics, Disablement, and Render Safe activities.

- Support the requirements as outlined in the Federal Radiological Emergency Response Plan (FRERP), the Atomic Energy Act, Title 40 and Title 44 of the Code of Federal Regulations, DOE Order 5530.2 for the Accident Response Group (ARG), DOE Order 5530.3 for the Radiological Assistance Program (RAP), DOE Order 5530.4 for the Aerial Measuring System (AMS), and DOE Order 5530.5 for the Federal Radiological Monitoring and Assessment Center (FRMAC).

Performance Measures

- Demonstrate improvement of a comprehensive emergency management system to ensure effective Departmental response to all DOE emergencies.

- Maintain robust emergency response assets in accordance with Presidential Decision Directives 39, 41, 62, 63 and 67; the Atomic Energy Act, Executive Order 12656; and Federal Emergency Plans.

- Conduct twelve (l2) emergency management system training and technical assistance conferences and workshops.

- Conduct six (6) emergency management system technical assistance visits.

- Conduct six (6) evaluations of Department-wide drills and exercises.

- Conduct six (6) appraisals of Departmental emergency programs.

- Conduct thirty-five (35) weeks of testing at the HAZMAT Spill Center.

- Provide situation assessments within one (l) hour after identification of a potential emergency.

Support the increased role and visibility of the Department as a leader in the formulation of National Security related policies for combating terrorism and nuclear materials trafficking.

Continue to evaluate and validate mission and operational readiness of the DOE emergency response assets through normal day to day operations. In FY 2001 each asset will participate in exercises, drills and training events. These activities will be evaluated to measure their needs and requirements to ensure full readiness.

Maintain the readiness of the response assets; and train staff to validate their ability to meet the current nuclear terrorist threat. These events will ensure that the assets maintain /test their technical capability, can respond quickly, and effectively coordinate and communicate with other Federal government agencies.

Maintain a training and readiness program to allow the Department of Energy to better assess the capabilities of the national assets, ensure coordination with local and state agencies, and identify and correct deficiencies in support of the United States national technical response and counterterrorism programs.

Significant Accomplishments And Program Shifts

Planning and Preparedness

Conducted emergency management system appraisals and evaluated Department-wide drills and exercises.

Continued customer involvement in planning, preparedness, and readiness assurance activities.

Continued collaborative efforts with Federal, state, tribal and industry entities to prepare for and respond to emergencies involving Departmental operations and activities.

Maintained the Headquarters emergency operations center voice, data, and video connection with DOE sites and other Federal agencies.

Training and Outreach

Improved operation of DOE's emergency management system and emergency facilities through technical assistance and enhanced training and assistance workshops.

Provided training to the Counter Terrorism Community on national security activities involving weapons of mass destruction.

Provided assistance to the Russian Federation Ministry of Atomic Energy in the development of a Situation and Crisis Center (Emergency Operations Center) at Minatom Headquarters in Moscow.

Response

Provided situation reports and assessments for developing emergencies.

Provided assessments of threats to DOE facilities and interests, and collaborated with the FBI's National Center for the Analysis of Violent Crime for joint information and data sharing.

Provided rapid credibility assessment of any nuclear threats involving nuclear weapons, devices or materials, and supported rapid credibility assessment of potential nuclear weapons or materials smuggling activities.

Provided, through the Atmospheric Release Advisory Capability Program, plume modeling and dispersion for radioactive material and chemical agent releases to the atmosphere.

Counterterrorism

Provided an annual report on illicit nuclear material transactions.

Continued supporting other U.S. Government agencies in combating nuclear terrorism and providing crisis and consequence management in response to any terrorist act.

Continued leadership role of the Department in the formulation of national security related policies for nuclear materials trafficking.

Funding Profile

(dollars in thousands)

	FY 1999 Current Appropriation	FY 2000 Original Appropriation	FY 2000 Adjustments	FY 2000 Current Appropriation	FY 2001 Request
Emergency Management					
Operating Expenses	16,000 [a]	16,000 [a]	-75 [c]	15,925	16,000
Emergency Response					
Operating Expenses	76,200 [b]	77,600	-5,860 [bc]	71,740	77,600
Sub-Total, Emergency Management	92,200	93,600	-5,935	87,665	93,600
Use of Prior Year Balances	-522				
General Reductions		-5,586	+5,586	0	
Total, Emergency Management . . .	91,678	88,014	-349	87,665	93,600

Public Law Authorization:
P.L., 83-703, "Atomic Energy Act of 1954"
P.L., 103-62, "Government Performance Results Act of 1993" [c]

[a] Transferred $5 million for the Communicated Threat Assessment activity to Nonproliferation and National Security' Office of International Materials Protection and Emergency Cooperation from the Office of Security and Emergency Operations' Office of Emergency Management.

[b] The amount shown is adjusted by $5.586 million for general reductions. The reduction is currently under review within the Department.

[c] Reflects 0.38% rescission -- $75 thousand in Emergency Mgt. and $274 thousand in Emergency Response.

Capital Operating Expenses & Construction Summary

Capital Operating Expenses

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$Change	%Change
Operation of HAZMAT Spill Center	1,500	1,500	1,500	0	0%
Total, Capital Operating Expenses	1,500	1,500	1,500	0	0%

Funding by Site

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Chicago Operations Office					
Argonne National Laboratory	263	405	418	13	3.2%
Brookhaven National Laboratory	585	603	724	121	20.1%
Total, Chicago Operations Office	848	1,008	1,142	134	13.3%
Oakland Operations Office	253	287	405	118	41.1%
Lawrence Livermore National Laboratory	11,229	10,603	10,080	-523	-4.9%
Total, Oakland Operations Office	11,482	10,890	10,485	641	-3.7%
Idaho Operations Office	307	345	473	128	37.1%
Albuquerque Operations Office	12,415	11,420	12,588	1,168	10.2%
Los Alamos National Laboratory	9,033	9,267	9,640	373	4.0%
Sandia National Laboratory	4,807	4,845	5,129	284	5.9%
Pantex	295	195	384	189	96.9%
Total, Albuquerque Operations Office	26,550	25,727	27,741	2,014	7.8%
Nevada Operations Office	34,036	33,775	33,767	-8	0%
Richland Operations Office	337	377	498	121	32.1%
Pacific Northwest Laboratory	300	225	0	-225	-100%
Total, Richland Operations Office	637	602	498	-104	-17.3%
Savannah River Site	248	280	399	119	42.5%
Oak Ridge Operations Office	2,863	2,852	3,003	151	5.3%
Oak Ridge Institute for Science and Education	12,487	13,807	12,922	-885	-6.4%
Washington Headquarters	2,742	3,965	3,170	-795	-20.1%
Undistributed general reduction		-5,586[a]			
Sub-Total, Emergency Management	92,200	87,665[a]	93,600	5,935	6.8%
Less use of prior year balances	-522				
Total, Emergency Management	91,678	87,665[a]	93,600	5,935	6.8%

[a]The amount of the general reduction is under review within the Department.

Site Description

Brookhaven National Laboratory

Funding provides for technical support for the exercise and appraisal program and the Subcommittee on Consequence Assessment and Protective Actions, which provides technical recommendations on emergency response to radiological and hazardous materials to protect health and safety of workers and the public. Also supports radiological assistance to Federal, state, tribal, and local governments and the private sector in event of an incident involving radioactive materials.

Argonne National Laboratory

Funding is provided to maintain operational readiness of assets; to conduct exercises and training; and to ensure that the Radiological Assessment Program is capable of responding to Federal, state, tribal, and local governments and the private sector in the event of an incident involving radioactive materials.

Idaho Operations Office

Funding is provided to maintain operational readiness of assets; to conduct exercises and training; and to ensure that the Radiological Assessment Program is capable of responding to Federal, state, tribal, and local governments and the private sector in the event of an incident involving radioactive materials.

Oakland Operations Office

Funding is provided to maintain operational readiness of assets; to conduct exercises and training; and to ensure that the Radiological Assessment Program is capable of responding to Federal, state, tribal, and local governments and the private sector in the event of an incident involving radioactive materials.

Lawrence Livermore National Laboratory

Funding provides for nuclear materials smuggling/trafficking/forensics program to develop capability to determine origin of stolen/smuggled nuclear materials and for Atmospheric Release Advisory Capability which provides plume modeling for emergency events, a critical element for the protection of workers and public. Funding also supports the Nuclear Emergency Search Team/Joint Technical Operations Team, and maintains and provides other emergency response assets as required.

Los Alamos National Laboratory

Supports the Emergency Operation Center system, connecting Operations Offices, laboratories, and relevant other Federal agencies by voice, video, and data to ensure cohesive and effective response to emergencies and support of counter terrorism activities. Funding also supports the Nuclear Emergency Search Team/Joint Technical Operations Team and maintains and provides. other emergency response assets as required.

Pantex Plant

Funding provides for Joint Technical Operations Team, and maintenance of other emergency response assets as required.

Nevada Operations Office

Funding provides for the HAZMAT Spill Center, a research and demonstration facility available on a user-fee basis to private and public sector test and training sponsors concerned with safety aspects of hazardous materials; continues emergency management activities including specialized training for DOE and stakeholders in subject areas such as weapons of mass destruction; and for the maintenance, upgrade and expansion of the Emergency Communications Network.

Richland Operations Office

Funding to conduct emergency management training activities to ensure comprehensive response to the spectrum of possible emergencies across the DOE complex and for radiological assistance to Federal, state, tribal, and local governments and the private sector in the event of an incident involving radioactive materials.

Pacific Northwest Laboratory

Funding provides for the SPIRE program (Spatial Paradigm for Information Retrieval and Exploration) to apply state-of-the-art analytical tools providing rapid understanding of large textual databases and for emergency management assistance for technical reviews and appraisals of the Department's emergency management system.

Savannah River Site

Funding is provided to maintain operational readiness of assets; to conduct exercises and training; and to ensure that the Radiological Assessment Program is capable of responding to Federal, state, tribal, and local governments and the private sector in the event of an incident involving radioactive materials.

Oak Ridge Operations Office

Funding provides for technical expert assistance for emergency management system appraisals and training development; for the behavioral assessment program to determine credibility of communicated threats; for the Emergency Management Issues Special Interest Group program, which provides training and information to emergency managers from across the DOE complex; and for radiological assistance to Federal, state, tribal, and local governments and the private sector in the event of an incident involving radioactive materials; and maintains and provides other emergency response assets as required.

Oak Ridge Institute for Science and Education

Funding supports the Nuclear Emergency Search Team.

Washington Headquarters

Funding provides for Emergency Operations Center and Communications Center maintenance and support; the support service contractor for Emergency Operations Center and Communications Center; and for maintenance and expansion of communications systems connecting the DOE complex and selected Federal agencies. The Emergency Operations Center and Communications Center are essential for Departmental response to emergencies that may occur at DOE facilities, elsewhere in the United States, and in foreign countries when assistance is requested. Funding for the Nuclear Emergency Search Team; Accident Response Group; Atmospheric Release Advisory Capability; Aerial Measuring System; Radiological Assistance Program; Federal Radiological Monitoring and Assessment Center; and the Radiological Emergency Assistance Center and Training Site.

Albuquerque Operations Office

Funding for the Nonproliferation and National Security Emergency Management Academy to ensure consistent and uniform emergency management training throughout the Department and for radiological assistance to federal, state, tribal, and local governments, and the private sector in the event of an incident involving radioactive materials; and provides for other emergency response assets as required.

Sandia National Laboratories

Funding supports counter terrorism activities; the exercise and evaluation program; and the Nuclear Emergency Search Team/Joint Technical Operations Team; and provides for other emergency response assets as required.

Operating Expenses

Mission Supporting Goals and Objectives

The Office develops and implements specific programs, plans and systems to minimize the impact of emergencies on national security, worker and public safety, and the environment. The Office provides overall coordination and consultation regarding the Department's Emergency Operations System. This includes emergency assistance and mobilization under the Federal Response Plan to radiological and non-radiological hazardous materials events, or in the event of malevolent threats or nuclear materials smuggling. The Office promulgates Departmental requirements and implementing guidance, and conducts readiness assurance activities to ensure an effective emergency operations system is in place at Departmental facilities. The Office also coordinates inter-agency and intra-Departmental emergency planning, preparedness and exercises, and coordinates with state and local governments, international agencies, foreign governments, and industry on emergency planning, preparedness and exercise issues.

The Office operates and maintains the Headquarters 24-hour per day emergency operations facilities and 24-hour communications center for the collection and processing of information relative to emergency notifications. In addition, the Office is responsible for reporting on and support of Headquarters emergency management activities and implementing a security program for the protection of office information, equipment, and facilities.

Office activities are in support of the Atomic Energy Act of 1954, as amended, Presidential Decision Directives 39, 41, 62, 63, and 67, Executive Orders 12656 and 12919, the Defense Production Act of 1950 as amended, Presidential Review Directive 47, and environment related regulations including the Resource Conservation and Recovery Act, Superfund Amendments and Reauthorization Act of 1986, Comprehensive Environmental Response Compensation and Liability Act, and Clean Air Act Amendments of 1990.

The Radiological/Nuclear Accident Response Program provides the capability for DOE to immediately respond to radiological accidents/incidents worldwide. This program provides overall program management and organizational structure during both emergency and non-emergency conditions for the personnel, equipment, and activities that collectively comprise the response capability. The emergency response assets are staffed primarily by engineers, scientists, other technical personnel from the national laboratories and production facilities, and other DOE management and operating contractors supporting the nuclear weapons complex. The funding for this program is allocated to 15 nationwide Department locations with the Nevada and Albuquerque Operations Offices, the Los Alamos National Laboratory (LANL), the Lawrence Livermore Laboratory (LLNL), and the Sandia National Laboratories (SNL) receiving the majority of the funding.

Funding Schedule

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$ Change	%Change
Emergency Management . . .	16,000 [b]	15,925 [a b]	16,000 [b]	75	0.5%
Radiological/Nuclear Accident Response	76,200	71,740[c]	77,600	5,860[c]	8.2%
Sub-total	92,200	87,665	93,600	5,935	6.8%
Use of Prior Year Balances	-522				0%
Total	91,678	87,665	93,600	5,935	6.8%

Detailed Program Justification

	FY 1999	FY 2000	FY 2001

Emergency Management

#	Operate nation-wide voice, data, and video link-up of DOE Operations Offices and select National Laboratory emergency operation centers, and expand system to include additional laboratories, DOE sites, and relevant Federal agencies. Operate the 24-hour Watch Office and Communications Center.	4,700	4,625	4,700

[a]Reflects 0.38% rescission.

[b]Transferred $5 million for the Communicated Threat Assessment activity to Nonproliferation and National Security from the Office of Security's Office of International Materials Protection and Emergency Cooperation from the Office of Security and Emergency Operations' Office of Emergency Management.

[C]The amount shown is adjusted by $5.586 million for general reductions. The reduction is currently under review within the Department.

	FY 1999	FY 2000	FY 2001
# Conduct planning, training and readiness assurance activities to ensure effective implementation of the Department's emergency management system. Provide emergency management, assessment, and threat awareness training and assistance workshops to Departmental elements and Federal, state, local, and tribal governments. Develop new training to meet specific needs.	3,400	3,400	3,400
# Conduct technical assistance visits and exercise support to assist Departmental elements in determining program weaknesses and cost effective means for making improvements. Evaluate tests and exercises of Departmental programs to demonstrate effective emergency response. Write after-action reports with findings and recommendations for all emergency situations and exercises involving Office of Emergency Management Staff and ensure follow-up of appropriate corrective actions to enhance the emergency management system.	2,200	2,200	2,200
# Continue the Department's support for crisis and consequence management in combating terrorism and nuclear material trafficking. Initiate a program in support of interagency and Departmental exercises to ensure adequate and comprehensive response to counter terrorism.	1,300	1,300	1,300
# Integrate the Atmospheric Release Advisory Capability (ARAC) plume modeling for chemical and hazardous materials releases involving Departmental activities.	600	600	600

	FY 1999	FY 2000	FY 2001
HAZMAT Spill Center			
# Continue user-sponsored spill tests for both government and industry at the HAZMAT Spill Center; provide spill test results to Departmental elements, other government agencies, industry and the general public for use in hazards mitigation and emergency responder training programs	1,500	1,500	1,500
Emergency Operations Support Service Contract			
# Staff the 24-hour Watch Office and Communications Center.	2,300	2,300	2,300
Total, Emergency Management	16,000 [a]	15,925 [a b]	16,000 [a]
Emergency Response			
Nuclear Emergency Search Team			
# Provides the U.S. Government's technical response to an act of nuclear terrorism. NEST is directed by DOE Headquarters and utilizes the expertise throughout the weapons complex, i.e., LANL, LLNL, SNL, Nevada Operations Office, Oak Ridge Institute for Science and Technology, and the Pantex Plant	43,816	44,965 [b]	44,205
Federal Radiological Monitoring and Assessment Center			
# FRMAC is a single source of compiled and quality controlled radiological monitoring and assessment data for any Federal agency, State, Tribal or local authority involved in resolving a radiological incident. FRMAC is managed by the Nevada Operations Office	1,217	1,217	1,582

[a]Transferred $5 million for the Communicated Threat Assessment activity to Nonproliferation and National Security's Office of International Materials Protection and Emergency Cooperation from the Office of Security and Emergency Operations' Office of Emergency Management.

[b]Reflects the 0.38% rescission.

	FY 1999	FY 2000	FY 2001
Atmospheric Release Advisory Capability			
# ARAC, located at LLNL, provides rapid predictions and projections of the dosage and amount of radio nuclides potentially transported, diffused and/or deposited into the atmosphere and the resulting impact on people and the environment	5,701	4,846	4,265
Aerial Measurement System			
# AMS, located at the Nevada Operations Office, is an aerial detection system capable of measuring gamma radiation for locating and tracking airborne radiation.	9,980	9,980	9,980
Accident Response Group			
# ARG, managed by the Albuquerque Operations Office, is responsible for the resolution of accidents or significant incidents involving U.S. nuclear weapons.	12,084	12,084	12,084
Radiological Emergency Assistance Center/Training Site			
# REAC/TS, located in Oak Ridge, provides medical advice, specialized training, and on-site assistance, in the treatment of all types of radiation exposure accidents.	974	1,174	1,409
Radiological Assistance Program			
# RAP provides a local capability and first response to requests for assistance during a radiological accident or incident. There are eight RAP regions: Brookhaven Area Office, Oak Ridge Operations Office, Savannah river Operations Office, Albuquerque Operations Office, Chicago Operations Office, Idaho Operations Office, Oakland Operations Office, and Richland Operations Office	2,288	2,860	3,575
Special Applications			
# Provides for classified activities and exercises associated with the seven emergency response assets; includes costs associated with Technical Integration activities that are crosscutting to the emergency response assets, and contractor support to achieve projected objectives related to the NEST and ARG activities	140	200	500
Undistributed general reduction.		-5,586	

	FY 1999	FY 2000	FY 2001
Total, Emergency Response	76,200	71,740 [a]	77,600
Use of Prior Year Balances	-522		
Total, Office of Emergency Management	91,678	87,665	93,600

Explanation of Funding Changes From FY2000 to FY2001

	FY2000 vs. FY 2001
Emergency Management	
# Provides modest adjustment to Communications Center activities	+75
Nuclear/Radiological Emergency Response	
# Adjustment to begin providing escalation	+274
Energy Response	
# Restore critical funding for Emergency Response to the FY 2000 request level	+5,586
Total Funding Change, Office of Emergency Management	+5,935

[a]Appropriated under Radiological /Nuclear Accident Program in the Weapons Activity account. The amount shown is adjusted by $5,586 million as a general reduction. Decreasing the adjustment is currently under review within the Department.

Nuclear Safeguards and Security

Program Mission

The Nuclear Safeguards and Security Program provides effective policy, programmatic direction and training for the protection of the Department of Energy's (DOE) nuclear weapons, nuclear materials, classified information, and facilities. The program provides technology development and technical support to domestic safeguards and security activities as well as implementation of effective classified information and information control policies, accounting and control of nuclear material in the U.S. Government, and the development of policy for and protection of cyber assets. The program will help ensure protection of the energy infrastructure against both physical and cyber attacks.

Program Goal

Support the National Security of the United States by assuring the effective, cost-efficient protection of the DOE's nuclear weapons, nuclear materials, classified information, and facilities against theft, sabotage, espionage, and terrorist activity. Fulfill DOE’s responsibility to develop and implement a plan with industry to assure the nation’s energy infrastructure.

Program Objectives

- Strengthen support to field elements to facilitate implementation of cost-saving safeguards and security measures.

- Develop Department-wide strategic and long-range planning for domestic nuclear safeguards and security.

- Modernize safeguards and security management information systems.

- Provide a domestic technology and systems development program to ensure the availability of state-of-the-art technical capabilities for the protection of sensitive DOE facilities, special nuclear materials, and national security interests including classified matter.

- Ensure availability of state-of-the-art technical capabilities for accountability and control of nuclear material recovered from disassembled nuclear weapons returned from the stockpile and storage of special nuclear materials.

- Support the role of the Safeguards and Security Nonproliferation and National Security Institute (formerly the Central Training Academy).

- Develop programs to support the standardization and accreditation of physical security systems.

- Protect national security while providing public access to DOE information.

- Provide leadership in jointly assessing sector vulnerabilities, recommending remedial plans, and developing systems and plans for identifying, countering, and recovering from attacks.

- Build an effective partnership between government and infrastructure owners and operators, with increased sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies.

- Educate and inform decision-makers and private industry, government, and the general public about infrastructure assurance, especially the importance of protecting their own information.

- Protect DOE nuclear facilities, employees and environment by providing a counterterrorist capability to detect and assess adversarial use of nuclear/chemical/biological weapons of mass destruction.

- Provide an effective system for the tracking and management of foreign visits by the Department of Energy that is supportive of rapidly changing and growing national security needs.

Performance Measures

- Through the Nonproliferation and National Security Institute, conduct 155 safeguards and security training courses with approximately 190 iterations (course repetitions) to protect domestic safeguards and security resources.

- Modify current technologies for safeguards and security applications or develop new technologies to reduce the backlog of documented and validated field user needs by about 41%.

- Continue the classification guidance streamlining initiative, issuing additional guides in the streamlined format.

- Collaborate with energy industry in four vulnerability assessments, using risk-based analytical tools, and develop “best practices” methodology.

- Conduct research and development program to identify and assess the vulnerabilities caused by interdependencies of national infrastructures.

- Implement baseline cyber security architecture at 12 sites.

- Provide cyber education, awareness, and training to all individuals responsible for implementing cyber security programs at DOE sites.

Significant Accomplishments and Program Shifts

- In FY 1999 and FY 2000, funding for the Nuclear Safeguards and Security program was appropriated in the Nonproliferation and National Security budget. As a result of the DOE-wide security reform announced on May 11, 1999, the Nuclear Safeguards and Security program was transferred to the

new Office of Security and Emergency Operations. Beginning with FY 2001, funding for this program will be budgeted for in the new Office of Security and Emergency Operations budget request.

- The Nuclear Materials Management and Safeguards System was transferred from the Office of Arms Control and Nonproliferation to the Office of Security Affairs. In FY 1999 and FY 2000, this program was appropriated in the Defense Program budget. However, for comparability purposes, FY 1999 and FY 2000 funding for this activity is reflected in this budget request.

- The development of advanced safeguards and security technologies have resulted in millions of dollars in savings and cost avoidance for the Department. The following are some examples of technologies that are planned to be implemented around the DOE complex: the Rapid Deployment Intrusion Detection system will provide a portable integrated, intrusion detection system; deliver the multi-platform trusted copy product to DOE sites to provide an authorized method to transfer unclassified text files from classified to unclassified IBM compatible personal computers; provide a portable measurement tool for gross nuclear material mass determinations; implement matrix correction techniques that provide accurate measurement of large crates to prevent smuggling of special nuclear materials (SNM); deliver a miniature, spectrometer, real-time sensor for detection of SNM and other property for use at vehicle and pedestrian portals to prevent theft or diversion of SNM; and implement a Compton suppression system based upon digital signal processing techniques that will significantly reduce the time it takes to make nuclear materials accountability measurements and thus reduce personnel radiation exposures as well as the time nuclear material sources have to be handled.

- The Safeguards and Security program has been and will continue to be the key deterrent in preventing major incidents (i.e., theft, sabotage, terrorist activity, etc.) across the complex at 16 domestic weapons sites.

- Enhanced training technology applications and applied a broader range of technologies to Departmental training, i.e., expanded use of interactive television, mobile training team, and televideo conferences to provide requisite training for a larger number of students without funding increases.

- The Classification/Declassification program has played a key role in protecting our national security posture by identifying which information warrants protection in the interest of the nation's security, while at the same time providing public access to information which does not warrant protection. The nation's security is preserved and the public's trust is being rebuilt through implementation of this program. In FY 1999 and FY 2000, funding for support service contracts supporting this program was provided in the Program Direction budget. In FY 2001, funding for this activity is budgeted in the Nuclear Safeguards and Security budget. However, for comparability purposes, FY 1999 and FY 2000 funding for this activity is reflected in this budget's request.

- The DOE Information Security program continues support in analyzing and deterring major incidents involving the compromise of classified information. This includes expansion of information assurance forensics analysis capabilities to support investigations and prosecutions of unauthorized disclosures of classified information, expansion of the technical surveillance countermeasures program, and

providing input into the information security technology development program to develop new technology in response to growing concerns over unauthorized disclosures of classified information.

In FY 1999, the Department reorganized the cyber security program by combining the classified and unclassified computer security programs within the Office of the Chief Information Officer. The Cyber Security Office has developed and issued risk management based policies for the protection of both classified and unclassified information. Additionally, an expanded cyber security training effort was initiated, the incident response capability (Computer Incident Advisory Capability) was enhanced, and work was initiated on a Public Key Infrastructure strategy and the development of core cyber security architecture methodology and requirements.

In FY 1999, the Department created the Office of Critical Infrastructure Protection to direct DOE's responsibilities under Presidential Decision Directive 63 to work with industry to develop and implement a plan to protect against, mitigate, respond to, and recover from attacks that would significantly disrupt the nation's energy infrastructure. The Office of Critical Infrastructure Protection is part of a Presidential crosscut coordinated by the Office of Science and Technology Policy.

Funding Profile

(dollars in thousands)

	FY 1999 Current Appropriation	FY 2000 Original Appropriation	FY 2000 Adjustments	FY 2000 Current Appropriation	FY 2001 Request
Nuclear Safeguards and Security					
Operational Support	31,230	32,816	-221[a]	32,595	47,216
Technology and Systems Development	24,620	27,470	-25[a]	27,445	25,970
Classification/Declassification	10,213	16,667		16,667	20,884
Cyber Security	0	9,318	+4,000[b]	13,318	30,339
Subtotal, Nuclear Safeguards and Security	66,063	86,271	+3,754	90,025	124,409
Use of Prior-Year Balances	-489[c]				
Less Use of Proposed Supplemental			-4,000[b]	-4,000	
Total, Nuclear Safeguards and Security	65,574	86,271	-246	86,025	124,409

Funding by Site

[a]Reflects Government-wide rescission of $246,000 in the Consolidated Appropriations Act.

[b]Proposed Supplemental Request.

[c]Reflects EWD reduction for use of prior year uncosted balances assigned to this program.

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Albuquerque Operations Office					
Los Alamos National Laboratory	8,048	6,688	8,244	1,556	23.3%
Sandia National Laboratories	8,135	9,718	11,233	1,515	15.6%
Pantex	0	20	0	-20	-100.0%
Albuquerque Operations Office	7,813	8,784	8,920	136	1.5%
Total, Albuquerque Operations Office	23,996	25,210	28,397	3,187	12.6%
Ohio Field Office		100	100	0	0
Chicago Operations Office					
Argonne National Laboratory	103	1,310	2,640	1,330	101.5%
Brookhaven National Laboratory	800	0	250	250	100.0%
Total, Chicago Operations Office	903	1,310	2,890	1,580	120.6%
Idaho Operations Office	822	1,187	1,437	250	21.1%
Nevada Operations Office	550	1,216	1,825	609	50.1%
Oak Ridge Operations Office					
Oak Ridge Operations Office	2,056	3,435	3,035	-400	-11.6%
Oak Ridge Institute for Science and Education	563	500	500	0	0
Total, Oak Ridge Operations Office	2,619	3,935	3,535	-400	-10.2%
Richland Operations Office	2,237	5,167	4,987	-180	-3.5%
Oakland Operations Office					
Lawrence Livermore Laboratory	8,637	13,676	13,945	269	2.0%
Savannah River Site	600	1,743	1,868	125	7.2%
Washington Headquarters					
Office of Scientific and Technical Information	40	105	100	-5	-4.8%
Washington Headquarters	25,659	36,376	65,325	28,949	79.6%
Total, Washington Headquarters	25,699	36,481	65,425	28,944	79.3%
Subtotal, Nuclear Safeguards and Security	66,063	90,025	124,409	34,384	38.2%
Use of Prior Year balances	-489				
Use of Proposed Supplemental.		-4,000		4,000	
Total, Nuclear Safeguards and Security	65,574	86,025	124,409	38,384	44.6%

Site Description

Los Alamos National Laboratory

Work at Los Alamos National Laboratory (LANL) is designed to address current, evolving, and future needs, primarily in the areas of materials control and accounting (MC&A) and information security. Activities in MC&A include the development of measurement technologies and instrumentation to quantify difficult-to-measure or shielded special nuclear materials. LANL also develops standards for special nuclear materials to calibrate instruments around the complex. Other activities include evaluating commercial measurement systems and the development of MC&A training. Information security efforts are focused on developing a capability to perform classified processing across multiple platforms and participation in the tri-laboratory effort to automatically detect suspicious activities on computer networks and automatically provide a response capability. Support is also provided to the Classification/Declassification program through the development and streamlining of classified guidance.

Sandia National Laboratory

Sandia focuses on development of technologies and systems required to protect the Department from catastrophic consequences such as use of nuclear energy for malevolent purposes or the erosion of national security secrets through theft or diversion of classified materials or information. Technical assistance is provided for assessment of site vulnerability analysis and site safeguards and security plans. Support is also provided for the Declassification Productivity Initiative by providing automated tools that improve the efficiency of document classification/declassification reviews. The technology development program focuses on physical security technologies to secure the DOE complex. Activities include providing new detection capabilities to automatically detect unauthorized access, explosives, or other contraband. Sandia will develop advanced barrier technologies to prevent or substantially delay attacks. Technological solutions will also be provided to address new threats, such as chemical and biological weapons. In addition, Sandia will continue to maintain a core technical capability in interior and exterior sensors, alarm communications, access delay, and entry control. Computer security activities include participation in the tri-laboratory effort to automatically detect suspicious activities on computer networks and automatically provide a response capability. Assistance is also provided in developing comprehensive classification guidance for nuclear safety, ES&H, and dismantlement/reuse; reviewing declassification proposals; and updating nuclear weapons classification guidance.

Pantex

Support was provided for the classification/declassification initiative by reviewing and releasing numerous documents prepared by the Amarillo National Resource Center for Plutonium (ANRCP). This also included classification training given to all cleared ANRCP employees.

Albuquerque Operations Office

The Nonproliferation and National Security Institute (NNSI), formerly called the Central Training Academy, is located in Albuquerque, New Mexico. NNSI was established to assist Headquarters DOE identify, implement, standardize, and monitor training programs in support of the Office of Safeguards and Security's program mission. NNSI's training curriculum, which consists of five core program elements (program management, personnel security, protection program operations, information security, and materials control and accountability), uses both traditional and distance learning technologies to provide onsite and facility training for safeguards and security personnel. The Classification/ Declassification program is supported by developing computer-based training for certifying classifiers and declassifiers.

Ohio Field Office

The Ohio Field Office supports the Classification/Declassification program by conducting a large-scale declassification review program to ensure that all documents are properly classified or declassified prior to the scheduled closure of the facility in FY 2004.

Argonne National Laboratory

Argonne provides technical and programmatic development assistance in support of DOE's initiative to establish an effective national infrastructure assurance program that is supportive of, and harmonized with, national infrastructure assurance efforts. Argonne also supports database development for tasks associated for foreign ownership, control, or influence operations facilitating a database of information that ensures more thorough DOE investigation. Support is also provided for the Declassification Productivity Initiative by providing automated tools that improve the efficiency of document classification/declassification reviews.

Brookhaven National Laboratory

Brookhaven supports the technology development program in the area of material control and accounting to increase assurance regarding special nuclear materials and other fissile materials by developing measurement capabilities for fuel.

Idaho National Engineering and Environmental Laboratory (INEEL)

INEL provides Idaho-based field expertise, technical assistance, and engineering support for the development, review, evaluation, and implementation of security-related requirements to effectively meet DOE's goals and ensure cost-effective use of DOE dollars. This includes review and evaluation of security design requirements; engineering support for validation, justification, and site safeguards and security plan reviews; and development and refinement of security design criteria.

Nevada Operations Office

Activities will be conducted at the Remote Sensing Laboratory and the Special Technologies Laboratory. Activities will focus on evaluating existing and new measurement technologies to determine their feasibility at DOE sites. Efforts also include developing technologies to assist protective force personnel, including night vision goggles and investigating the use of ultraviolet tags to differentiate between the adversary and site personnel.

Oak Ridge, Lockheed Marietta Energy Systems

At Oak Ridge, technical assistance is provided for the development, maintenance, and conducting of courses and workshops that evaluate and ensure Information Systems Security certification; Master Safeguards and Security Agreement/Site Safeguards and Security Plan verification/validation; and physical protection systems. The technology development program support in physical security and material control and accounting addresses needs for protecting nuclear weapons, nuclear material, classified information, and other vital DOE assets (nonnuclear and unclassified). Expertise is provided in the document classification/declassification initiative and for classification guidance update and streamlining. The Classification/Declassification program is supported through development and streamlining of classification guidance.

Oak Ridge Institute for Science & Education/Oak Ridge Associated Universities

At Oak Ridge, technical support provides implementation, training, operation, and quality assurance of the Personnel Security Assurance Program, and a variety of research and analysis activities in support of the personnel security function.

Richland, Battelle Memorial Institute/Pacific Northwest National Laboratory (PNNL)

PNNL provides technical expertise, assistance, training, and awareness in support of information security. This includes the identification, inquiry, and resolution of security problems across DOE; and analysis of incidents and facility survey information. They also assist with the implementation of the Department's information assurance initiative and related activities to ensure effective and efficient identification of threats and vulnerabilities to DOE's distributed information and telecommunication systems. Technical assistance is provided that supports special nuclear material consolidation, Master S&S Agreement, Site S&S Plan support, and vulnerability assessment reviews and performance testing. The Classification/Declassification program is supported through development and streamlining of classification guidance.

Richland, Fluor-Daniel Hanford

Provides Hanford-based field expertise, technical support and assistance for the review, update and consolidation of safeguards and security orders and policies and field guidance to cost effectively meet department goals and objectives.

Lawrence Livermore National Laboratory (LLNL)

Technical support is provided to DOE's Information Systems Security Program for analysis and recommendations of policies, guidance, and information assurance tool development for all aspects of information systems security. The technology development program at LLNL is concentrated in information security, physical security, and materials control and accounting (MC&A). LLNL provides the Department with many tools to detect and respond to attacks to information system networks. The laboratory is also a participant in the tri-laboratory effort to automatically detect suspicious activities on computer networks and automatically provide a response capability. Physical security activities focus on providing software and interface upgrades to the Department's standardized access control system and evaluating low cost access control technologies for implementation throughout the DOE. In MC&A, measurement solutions for heterogeneous materials are being developed and implemented around the complex. Through the Computer Incident Advisory Capability (CIAC), provide round-the-clock cyber security incident response, analysis of cyber intrusions and attempted intrusions, and alert capability to DOE . Classification/declassification is supported through development and streamlining of classification guidance.

Savannah River Site

Work at Savannah River supports materials control and accounting through the enhancement, development, deployment, and operation of a fully developed, ready to use, software application for nuclear materials accounting throughout the DOE complex. This technology will allow for greater reliability, efficiency, and cost savings through increased standardization and use of advanced software technologies. The classification/declassification program is supported through the development and streamlining of classification guidance.

Office of Scientific and Technical Information

Support is provided for the classification/declassification initiative by improving the access capability to DOE's OpenNet data base and maintaining and enhancing the thesaurus and dictionary for the automated classification guidance system.

Washington Headquarters

The headquarters program for Nuclear Safeguards and Security has responsibility for implementation and oversight of the headquarters guard contract; the Safeguards and Security Information Management System (SSIMS) database; maintenance/upgrade of alarm systems, access control systems, and related computer equipment; and the protective force radio system; as well as the statutory-based responsibility for classifying and declassifying nuclear weapons-related technology (known as Restricted Data), ensuring that policies provide the public access to information necessary for an informed discussion of DOE's nuclear weapons program while continuing to support the paramount objective of protecting information from strategic adversaries, proliferants or potential proliferants, and terrorists. Specific areas covered are developing detailed classification guidance which specifically identifies information requiring protection in the interest of the national security; reviewing documents to classify information that still warrants protection and declassifying information that is no longer sensitive; training personnel both within DOE and throughout the Government to recognize Restricted Data information and to ensure that it is properly classified to prevent its inadvertent release; appraising DOE and other-agency classification

and declassification programs to ensure policies and procedures are applied consistently; and developing state-of-the-art technology to make the classification and declassification process more efficient and effective. Also, in support of the Cyber Security program, support services are required to provide support to the DOE Headquarters staff in developing DOE-wide policies and plans, training, and architecture design and implementation.

Operational Support

Mission Supporting Goals and Objectives

Safeguards and Security Operational Support provides essential technical and analytical expertise to ensure effective and efficient security; a protective force for Headquarters operations; reviews which ensure cost-saving measures in safeguards and security throughout the Department; and standardized training responsive to the challenges of the changing post-cold war era. This support provides for the overall improvement of safeguards and security activities.

Subprogram activities in this section of the budget include the following:

- **Nonproliferation and National Security Institute (NNSI) (formerly Central Training Academy)** is the Center of Excellence for safeguards and security training and training development. NNSI uses both traditional and distance learning technologies to provide onsite and facility training for safeguards and security personnel ensuring that DOE maintains a well-trained workforce to protect the nation's vital nuclear and energy interests against espionage, sabotage or theft. NNSI assesses safeguards and security field training needs and site training program performance and develops training courses to meet those needs. Distance Learning Training includes satellite transmission of NNSI training to multiple DOE sites and, through the use of modern interactive technology, allows each student to be part of the instructional process. Computer-based training, interactive audio/video training and correspondence courses are also provided.

- The **Nuclear Materials Management and Safeguards Systems (NMMSS)**, which tracks and analyzes U.S. and Foreign nuclear activity, was transferred in FY 1999 from the International Nuclear Safeguards subprogram in the Office of Arms Control and Nonproliferation to the Office of Plutonium, Uranium, and Special Material Inventory in the Office of Security Affairs. In FY 1999 and FY 2000, funding for NMMSS was provided within the Office of Arms Control and Nonproliferation. Beginning in FY 2001, NMMSS will be funded in the Nuclear Safeguards and Security budget.

- **Information Security** provides support across the department in the areas of classified matter protection and control; technical security; operations security; and foreign ownership, control or influence. The accelerated information assurance program will provide a capability for ensuring that the resources and methods necessary to identify and prosecute unauthorized intruders of Departmental networks are effective and available. The information security activities will also provide a capability to evaluate proposed security measures within the Department's complex environment. The Information Security Resource Center (ISRC) incorporates technical expertise and professional development training to ensure that the five disciplines of information security function in an integrated, cohesive manner. The Technical Surveillance Countermeasures (TSCM) program, which is one of the five disciplines, ensures and enhances the security provided for Departmental facilities and programs in the greater Washington, D.C. area. The Information Security Protection Program provides a vehicle for providing technical expertise, assistance, and awareness training in information security disciplines. The information security program provides matrix support to various Departmental programs, such as the critical infrastructure program, the counterterrorism/ counterintelligence programs, and the cyber security program.

- **Security Education Briefings and Awareness** provides support for Security Education Briefings and Awareness to reflect changing policies and procedures. Coordinates and participates in security education workshops and meetings for the exchange of resources and dissemination of security education information and assists contractors in establishing supporting briefing materials.

- **Personnel Security** evaluates, reviews, and develops guidance and documents for use in evaluating the Personnel Security Assurance Program (PSAP) as it relates to medical, psychological, legal, security, and management components. Researches and prepares technical documents to support the Personnel Security activities. Provides technical assistance and operational support to the Personnel Security program manager to determine current status of science and technology in the component areas.

- **Additional Support** provides Headquarters and field elements with support to implement cost-saving safeguards and security measures. This support includes technical assessments, risk management/vulnerability assessment expertise, engineering assistance, surveys, and performance testing. FY 1999 security risk management activities focused resources on systems modeling and protective force performance characterization. FY 2000 activities and funding levels were formulated to support risk management activities for high-value assets and to identify potential weaknesses and enhancements for protection systems and to incorporate lessons learned into the risk management processes. FY 2001 will support continuing risk management issue resolution and the incorporation of greater sensitivity and capability into current vulnerability assessment tools. Additional Support also provides technical support for the development of physical security policies and programs and the security alarm system at Headquarters.

  The Safeguards and Security Information Management System (SSIMS) tracks and reports classified safeguards and security issues from all DOE field sites. SSIMS allows the Office of Safeguards and Security to conduct continuous reviews of the security measures in place at DOE/contractor facilities, ensuring compliance with DOE policy requirements and monitoring the effectiveness of Departmental policy involving the protection of national security assets. SSIMS funding will maintain the current database information system detailing facility findings, ratings, and general operational status.

  The Headquarters Guard Contract provides security for the protection of Government property, classified matter, and personnel at headquarters buildings.

  Additionally, support is provided for the implementation of a nuclear/biological/chemical weapons equipment program across the DOE complex to provide protection to the protective forces from these weapons of mass destruction.

- **Critical Infrastructure Protection Program** will carry out the national mandates of the Critical Infrastructure Protection directive and Presidential Decision Directive 63 regarding critical infrastructure protection. These mandates obligate DOE to partner with the private sector in ensuring the viability of the energy sector infrastructures nationwide. In addition to responsibilities for its own critical infrastructure, the Department is primarily responsible for ensuring that the DOE national laboratories' capabilities are fully utilized in regards to developing flexible, evolutionary approaches that span both public and private sectors, and protect both domestic and international security.

- **#** The **Foreign Visits and Assignments Program** (FV&A) manages the Department-wide approval process for foreign nationals visiting or assigned to DOE federal and contractor (including National Laboratories) facilities for the purpose of conducting unclassified work. The FV&A Program: develops and disseminates the Department's policy and procedures; develops and implements the Department's central tracking information systems; develops and coordinates responses to external requests (e.g., Congress) for information on the substance and numbers of foreign nationals visiting or working throughout DOE; and provides oversight of field operations to ensure that national security needs are being effectively addressed by the conduct of actual operations.

Funding Schedule

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Nonproliferation and National Security Institute (NNSI)	7,813	8,677	8,665	-12	-.1%
Nuclear Materials Management and Safeguards System (NMMSS)	2,500	2,500	2,500	0	0.0%
Information Security	3,982	4,269	4,814	545	12.8%
Security Education Briefing and Awareness	181	181	172	-9	-5.0%
Personnel Security	485	485	431	-54	-11.1%
Additional Support					
Headquarters Guard Contract	7,000	7,654	9,000	1,346	17.6%
Other	9,269	5,729	7,509	1,780	31.1%
Total Additional Support	16,269	13,383	16,509	3,126	23.4%
Foreign Visits and Assignments Program	0	1,000	1,125	125	12.5%
Critical Infrastructure Protection Program	0	2,100	13,000	10,900	519.0%
Total, Operational Support	31,230	32,595	47,216	14,621	44.9%

Detailed Program Justification

	FY 1999	FY 2000	FY 2001
Nonproliferation and National Security Institute			
# Conduct approximately 155 courses with 190 classroom iterations, emphasizing "Online Training." Funding in FY 2001 allows the completion of course development that commenced in FY 2000 to meet identified field site training needs for Weapons of Mass Destruction, chemical/ biological equipment, and physical security systems. Funding will reduce accumulated deferred infrastructure maintenance/replacement by 18%, including fire alarms, Americans with Disability Act (ADA) upgrades, and fire sprinkler systems.	7,750	8,614	8,602
# Provides funding to support NNSI's equipment-related needs such as replacement of outdated online and interactive television equipment	63	63	63
Total, Nonproliferation and National Security Institute	7,813	8,677	8,665

	FY 1999	FY 2000	FY 2001
Nuclear Materials Management and Safeguards System (NMMSS)			
# Track and analyze U.S. and foreign nuclear activity to satisfy statutory requirements and international obligations. Serve as the states' system of accounting and control of nuclear material in the U.S. Government.	2,500	2,500	2,500
Information Security			
# The Information Security Resource Center (ISRC) in FY 2001 continues to provide technical expertise, assistance, training, and awareness in an integrated manner across the five disciplines of information security. This activity does not include cyber security functions. Activities support the identification of, inquiry into, and resolution of security problems across the Department, especially in the area of unauthorized disclosures and compromises of classified information; analysis of incidents and facility survey information to identify problems within the information security program; and analysis of foreign ownership, control or influence (FOCI) in determinations of contracts within the various program elements of DOE dealing in classified information. The funding level reflects the continuing need to sustain efforts to prevent unauthorized disclosures or compromises of classified information throughout DOE and the increasing complexity of FOCI issues.	1,152	1,602	1,602

	FY 1999	FY 2000	FY 2001
# The Information Security Protection Program (ISPP) in FY 2001 continues to provide technical advice and awareness (excluding cyber security) to Departmental entities. The ISPP provides unbiased capability in the areas of information security including technical vulnerability testing, design reviews to support the complex wide technical surveillance countermeasures program (TSCM), TSCM surveys and inspections at DOE sites not currently receiving such services, independent verification and validation of information security measures, TSCM equipment inspection support to international treaties, and awareness of emerging information security issues. ISPP activities provide a basic level of assurance that key assets are protected in a reasonable manner to ensure that national security concerns of the country are not adversely affected by adversary activities. Funding levels are based on attention to unauthorized disclosure of classified information and the conduct of TSCM services.	1,500	1,405	1,900
# Activities include expansion of information assurance forensics analysis capabilities to support investigations and prosecutions of unauthorized disclosures of classified information. Complete development of the Grey List data base which will allow contractors to submit foreign ownership, control or influence packages electronically, facilitating a data base of information that will ensure more thorough DOE investigation. Develop an internet accessible list of facility security offices for the over 2,000 cleared DOE facilities and a list of classified mailing addresses for the over 500 facilities that are authorized to receive classified matter. Funding levels have been determined based on the rate of technological advances and, in the case of forensics, based on similar activities within the Department of Defense.	1,000	1,100	1,150
# Provided for liaison to various departmental programs and missions including counterintelligence, counterterrorism, and internal critical infrastructure protection. In FY 2000, this effort was transferred to the Cyber Security program.	168		

	FY 1999	FY 2000	FY 2001
# Provides for continuation of on-site technical support for information security in the areas of technical reviews of technology transfer issues and the conduct of inquiries into unauthorized disclosures of classified information, emphasizing computer forensics.	162	162	162
Total, Information Security	3,982	4,269	4,814
Security Education Briefings and Awareness			
# Provide security awareness throughout the DOE complex through education programs			
# Support security awareness and education through information exchange by planning and conducting one Security Education Special Interest Group (SE/SIG) workshop			
# Maintain the SE/SIG electronic bulletin board	181	181	172
Personnel Security			
# Operate Center for Human Reliability Studies			
# Support personnel security activities through guidance and product development, update and revise 90% of anticipated personnel security materials			
# Serve as technical liaison with Department of Defense (DOD) Personnel Security Research Center, DOD, Polygraph Institute and similar agencies and institutions			
# Upgrade and maintain Personnel Security Assurance Program (PSAP) electronic bulletin board; evaluate and modify 80% of needed PSAP training materials	485	485	431
Additional Support			
# Headquarters Guard Contract - Ensure a sound protection program is offered to Headquarters employees and facilities through use of 40 static posts and roving patrols, 16 supervisors, 4 managers, and 20 instructors, receptionists and administrative assistants, executive protection personnel, armorer, and quality assurance, badging and technical countermeasures personnel. In FY 2001, funding includes arming 30% of personnel.	7,000	7,654	9,000
# Support operational and basic maintenance costs for the Safeguards and Security Information Management System (SSIMS) which tracks and reports classified safeguards and security issues from all DOE field sites.	300	300	300

	FY 1999	FY 2000	FY 2001
# In FY 2001, provides support and corrective/preventative maintenance of alarm systems, magnetometers, and metal detectors at both headquarters facilities. Also provides for engineering support, minor enhancements, and modifications to the headquarters access control systems and for vehicle barrier systems at both headquarters facilities	753	868	883
# Support the headquarters protective force radio system maintenance at the 90% operational level.	50	85	85
# Provide risk management, vulnerability assessment, and safeguards and security system performance evaluations, verifications, and validations. In FY 2001, additional protective force modeling and evaluation, and safeguards and security vulnerability assessments, based on enhanced vulnerability assessment tools, are necessary to address potential weaknesses and emerging threats	1,283	1,593	1,733
# Provide technical support for the development of physical security policies and programs. Evaluate the performance of integrated alarm management and control systems in the field to determine compliance with DOE directives, develop explosive detection performance evaluation test kits, revise DOE Definitions Guide, revise Protection Program Operations Survey Process, coordinate explosive detection technology workshops, and provide technical support in reviewing security system implementation at DOE sites . . .	387	387	387
# In FY 1999 and FY 2000, provided for the procurement and replacement of security locks meeting Federal Specification FF-L-2740A for containers holding sensitive classified material	1,000	1,000	
# In support of Congressional initiative for FY 2000, assess current vulnerability of security equipment throughout the DOE complex and develop solutions to identified vulnerabilities, i.e., evaluate current commercial security systems to determine applicability to DOE.		1,000	

	FY 1999	FY 2000	FY 2001
# Nuclear/Biological/Chemical Weapons (NBC) Protection Equipment, Training, and Chemical/Biological Detection Equipment - In response to U.S. Policy on Counterterrorism (PDD-39), provide a counterterrorist capability to detect, assess and protect Departmental facilities, employees and the environment from adversarial use of NBC as a weapon of mass destruction (WMD). Funding supports initial development and implementation of NBC programs across the DOE complex. This includes purchase of standardized NBC personal protection, assessment and decontamination equipment for protective forces (PF) at DOE sites, development/training for the PF, conduct of performance tests/exercises to validate NBC program effectiveness and readiness, multiagency coordinated NBC exercises, and development of complex wide NBC response programs and site-specific response plans and procedures. Funds also support initial efforts for development, purchase, and installation of NBC detectors for DOE facilities with Categories I and II Special Nuclear Material and nuclear weapons and other significant national security assets. Funding level was based upon extensive personal protection equipment testing, examination of lessons learned from the U.S. Marine Corps Chem-Bio Incident Response Force and the FBI Hostage Rescue Team chemical/biological program development. Project will help standardize protective force equipment and sustain exchangeability among DOE sites, significantly reducing DOE facilities' vulnerabilities to NBC threats through development and acquisition of sensors and chemical/biological and explosive detection equipment; increase PF effectiveness and performance level through training and exercising to mitigate the nuclear/ chemical/biological threat; and greatly enhance protection and assessment of key special nuclear material assets at critical nuclear facilities			3,625

	FY 1999	FY 2000	FY 2001
# Supports capitalized computer equipment requirements and modification and/or replacement parts to the Headquarters alarm and access control system. In FY 1999 work was initiated to begin alarm system replacement and installation of vehicle barrier systems at Headquarters for compliance with the Department of Justice Report on "Vulnerability Assessment of Federal Facilities."	5,496	496	496
Total, Additional Support	16,269	13,383	16,509
Foreign Visits and Assignments (FV&A) Program			
# Supports requirements resulting from PDD 61 directing the establishment of an Office of Foreign Visits and Assignments at DOE and increased attention and inquiry by the U.S. Congress: for improved management of visits and assignments by foreign nationals to DOE sites (including National Laboratories) nation-wide; to develop responsible program policies; for information concerning the number of foreign nationals visiting or assigned to DOE sites and the countries and the technologies involved; to develop analytical studies on FV&A; to perform oversight of program implementation effectiveness; to represent the DOE in related internal and external fora; and for required increases in critical program, technical, and automated information capabilities to collect and analyze data, (e.g., the Foreign Access Records Management System (FARMS)) to maintain and provide reliable information to the Secretary and the Congress in an environment of rapidly changing and growing security needs. The increased funding in FY 2001 supports the direction in Section 3146 of the FY 2000 Defense Authorization Act for DOE to increase examination of visits and assignments by foreign nationals from selected countries to the national weapons laboratories as an extra level of security protection.		1,000	1,125

	FY 1999	FY 2000	FY 2001
Critical Infrastructure Protection Program (CIPP)			
# Infrastructure Assurance Outreach Program: Work focuses on developing an understanding of the vulnerabilities of operations of the very large, integrated, and complex electric power, natural gas, and oil systems and the relationship of information flows to operational capabilities. A related area of focus is concerned with high-security Supervisory Control and Data Acquisition (SCADA) systems to address the issues of secure communications, validation of commands, the development of design and operational guidelines, including authentication and authorization techniques to control access to energy system commercial information. FY 2001 activities will expand upon previous infrastructure assurance efforts (in electric power and, to a lessor extent, natural gas infrastructures) to work with utilities to identify and evaluate the threats to, and vulnerabilities of, the natural gas and oil infrastructures. This includes both cyber (information) and physical infrastructure components. One assessment of the natural gas infrastructure and three assessments of the oil infrastructure would be conducted at various utilities. A summary of lessons learned and recommended security practices for the energy industry would be developed.		800	1,500
# Infrastructure Interdependencies: The energy infrastructure is highly interdependent internally and with other infrastructures. This work will use modeling and simulation to characterize the interdependencies, quantify the impacts of vulnerabilities in each system on the others, and rank the order of importance of various interdependencies. Work will focus on developing demonstrating, and delivering analytic capabilities and supporting knowledge bases to significantly improve understanding of, and the ability to comprehensively study, the interdependent nature of the U.S. energy infrastructure. This will involve: (1) enhancing existing and developing new analytical tools that treat infrastructure interdependencies explicitly; (2) enhancing early alert screening tools that provide infrastructure stress indicators; (3) coordinating with Federal Agencies to link to models and simulations of other critical infrastructures; (4) enhancing existing and developing new policy and impact analysis tools; and (5) developing an integrated architecture for analyzing the technical, economic, and national security implications of energy technology and policy decisions. . . .		1,100	4,000

	FY 1999	FY 2000	FY 2001
# Energy Sector Outreach: Provides expert technical assistance to the Energy Sector Coordinators in establishing collaborative working relationships between the government and the energy industry and other stakeholders; facilitates development of information collection and sharing and assists in analyses.		200	200
# Critical Consequence Analysis and Management for the Energy Infrastructure: Develop the data, methodologies, and tools to evaluate the public health and safety, national security, and economic consequences of disruptions to energy infrastructures and the processes to assist in restoration and reconstitution.			2,000
# Evaluation of Policy Effects and Institutional Barriers: Evaluates the cause-and-effect relationships between specific public policies, institutional barriers, and energy infrastructure vulnerability.			600
# Development of Real-Time Control Mechanisms in the Energy Infrastructure: Identifies the vulnerabilities of real-time control systems and develops technologies that protect against unauthorized control of, or intrusion into the system.			600
# Risk Management Tools for the Energy Infrastructure: Develops tools to assist decision makers in planning and implementing protection and mitigation strategies, and for predictive risk management allowing for real-time, accurate interpretation of system monitoring information.			800
# Analysis of Scale and Complexity of the Energy System: Research characterizing the internal dynamics of large, complex, non-linear energy infrastructure focusing on stability, countermeasures, complexity reduction, uncertainty effects, and personnel behavior.			1,200

	FY 1999	FY 2000	FY 2001
# Development of Integrated Multi-Sensor and Warning Technologies for the Energy Infrastructure: This research is focused on the development of an integrated, corroborative system of overlapping technologies, including sensors, designed to warn of attacks and impending failures at critical points in the energy system. The focus would be on tamper detection and failure warning technologies such as acoustic instrumentation, electronics signals, video imaging, satellite oversight, remote methane detection (hand-held and airborne), expert system data interpretation, and standards development. Advanced technology approaches and cost reduction will be the focus of the Federal R&D.			1,700
# Geomagnetic Interference warning systems: Develop a methodology that would enable electric power system operators to establish emergency operations procedures for electric power systems under the influence of intense geomagnetic disturbance. This will provide a cost-effective approach to reduce power system vulnerability to predictive increases in sunspot activity in the next few years.			400
Total, Critical Infrastructure Protection Program	0	2,100	13,000
Total, Operational Support	31,230	32,595	47,216

Explanation of Funding Changes from FY 2000 to FY 2001

	FY 2000 vs. FY 2001 ($ 000)
Nonproliferation and National Security Institute	
# Reflects reduced emphasis on maintenance/replacement upgrades of existing infrastructure	-12
Information Security	
# Development of internet accessible list of facility security offices for over 2,000 cleared DOE facilities and list of classified mailing addresses for over 500 facilities authorized to receive classified matter	+50
# The conduct of technical surveillance countermeasures surveys and inspections at DOE sites not currently receiving such services	+495
Security Education Briefings and Awareness	
# Reduces the number of workshops on the Security Education Special Interest Group to one a year	-9
Personnel Security	
# Update and revise 90% of personnel security materials and 80% of needed PSAP training materials	-54
Additional Support	
# Arming 30% of protective force personnel and minor enhancements to headquarters access control systems	+1,361
# Increased protective force modeling and evaluations and S&S vulnerability assessments to address potential weaknesses and emerging threats	+140
# Reflects reduction for FY 2000 funding for procurement of security locks that meet Federal Specification FF-L-2740A and assessing the vulnerability of security equipment throughout DOE	-2,000
# In response to U. S. policy on counterterrorism, supports the initial implementation of nuclear/chemical/biological (NBC) programs across the DOE complex by providing NBC protection equipment, training, and chemical/biological detection equipment	+3,625
Foreign Visits and Assignments Program	
# Supports requirement of Section 3146 of the FY 2000 Defense Authorization Act that DOE increase examination of visits and assignments by foreign nationals from selected countries to the national weapons laboratories as an extra level of security protection.	+125
Critical Infrastructure Protection	
# Expand infrastructure assurance efforts to work with utilities in identify and evaluating threats to, and vulnerabilities of, natural gas and oil infrastructures	+700

	FY 2000 vs. FY 2001 ($ 000)
# Enhance existing and develop new analytical tools that treat infrastructure interdependencies explicitly, enhance early alert screening tools that provide infrastructure stress indicators, and enhance existing and develop new policy and impact tools	+2,900
# Develop data, methodologies and tools to evaluate the public health and safety, national security, and economic consequences of disruptions to energy infrastructures and the processes to assist in restoration and reconstitution	+2,000
# Evaluate cause-and-effect relationships between specific public policies, institutional barriers, and energy infrastructure vulnerability	+600
# Develop real-time control mechanisms for identified vulnerabilities to protect against unauthorized control or intrusion of system	+600
# Develop risk management tools to assist in planning and implementing protection and mitigation strategies and for predictive risk management allowing real-time interpretation of system monitoring information	+800
# Perform research on scale and complexity of the energy systems focusing on stability, countermeasures, complexity reduction, uncertainty effects, and personnel behavior	+1,200
# Develop integrated multi-sensor warning technologies for the energy infrastructure focusing on tamper detection and failure warning technologies	+1,700
# Develop warning systems that would allow electric power system operators to establish emergency operations procedures for electric power systems under the influence of intense geomagnetic disturbance	+400
Total Funding Change, Operational Support	+14,621

Technology and Systems Development

Mission Supporting Goals and Objectives

The Technology and Systems Development program's mission is to develop new technologies or modify commercial systems to protect the National nuclear complex, special nuclear materials, classified information and other critical assets. The threats facing DOE facilities and sites continue to evolve and present many challenges to the Department. Traditionally, the Technology and Systems Development Program was concerned with nuclear material control and accounting, but now is faced with other threats including weapons of mass destruction, terrorism, cyber attacks and the insider. Although the Department is no longer in a production mode, it is disassembling nuclear weapons and has received weapons grade materials from other countries. All of these weapons grade components and materials have resulted in increased nuclear material inventories which the Department must properly account for and protect. Technology continues to be the key to protecting and securing the Department's facilities and assets. Safeguards and Security deficiencies requiring technical solutions have been identified and validated by safeguards and security managers around the DOE complex. Currently, the Technology Program for Domestic Safeguards and Security can partially address approximately 41% of its domestic requirements. In addition, these deficiencies have been validated by independent tests by DOE contractors and have resulted in a shift of program funds from information security to physical security to address these documented vulnerabilities. The program continues to provide technical solutions to meet our customers' needs. The program will continue to strive to sustain and utilize core security technologies and expertise, but also provide technical defenses against chemical and biological terrorism, large bombs, and the significant potential threat posed by insiders with direct access to our protected assets.

The Technology and Systems Development program is divided into the following subprograms:

Science and Technology Development Projects includes all activities ranging from basic research to full scale development and modification of available technology for safeguards and security applications.

Technology Application includes site implementation of a technology or system that will address a safeguards and security deficiency, and technology transfer to a qualified manufacturer.

Technology Support, Assistance, and Consultation Tasks includes technical training, technical support to Headquarters, technical workshops and seminars, and technical support and assistance to the DOE complex.

Each subprogram is concentrated in the following disciplines:

Physical Security: Activities are focused on intrusion detection, access control, alarm control and display, alarm assessment, adversary barriers/delay, and protective force subsystems.

Material Control and Accounting: Efforts are focused in nuclear material measurements, material accounting, material control, training, and statistical control methods.

Information Security: Projects are focused on intrusion/attack detection tools, technical assistance, system integration, and information assurance.

Funding Schedule

(Dollars in Thousands)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Science and Technology Development Projects	19,877	24,129	24,400	271	1.1%
Technology Application	1,417	1,066	805	-261	-24.5%
Technology Support, Assistance, and Consultation Tasks	3,326	2,250	765	-1,485	-66.0%
Total, Technology and Systems Development	24,620	27,445	25,970	-1,475	-5.4%
Crosswalk of Disciplines					
Physical Security	9,318	11,128	13,275	2,147	19.3%
Material Control and Accounting	9,796	10,047	9,867	-180	-1.8%
Information Security	5,506	6,270	2,828	-3,442	-54.9%
Total	24,620	27,445	25,970	-1,475	-5.4%

Detailed Program Justification

	(dollars in thousands)		
	FY 1999	FY 2000	FY 2001
Physical Security			
# Develop solutions to known vulnerabilities at DOE sites. Increase provides for the accelerated development and implementation of solutions to known vulnerabilities, thus reducing the threat to DOE facilities and assets. (SNLA, LLNL, Remote Sensing Lab/NV, and OR/LMES)	3,258	3,665	4,390
# Provide required upgrades to the Department's standardized integrated alarm and access control system. Modernization efforts include replacing outdated software, adding new sensors, and simplifying the user interface. (LLNL)	950	1,450	1,450
# Test and evaluate explosives detection technologies to provide state-of-the-art knowledge to be applied as a defense across the DOE complex. Reduction is due to a shift in program priorities. (SNLA)	680	980	450
# Develop advanced protective force technologies to defend against adversaries using available weaponry. Increase provides a remote vital sign monitor for protective force personnel and a heads up display which enables special response team forces to fire weapons accurately from concealed positions minimizing body exposure to fire. The funding for this activity was previously included under the "Develop solutions to known vulnerabilities" (Special Technologies Laboratory, NV, LMES)	727	1,005	1,805
# Quantify performance of security systems to provide DOE sites with a single source for recommendations on the most effective security systems to implement. Decrease is a result of shifting funding to developing advanced barriers. (SNLA)	1,365	1,340	850
# Fund DOE's support to the National Interagency R&D Program for combating terrorism. (DOE-HQ)	750	750	750
# Evaluate/develop robust barriers or access delay technologies to counter advanced attack tools. Increase is provided to update the access delay technology transfer manual and to investigate new delay techniques. (SNLA)	450	650	1,050
# Provide technical assistance and maintenance to DOE sites for physical security requirements.			1,000

	(dollars in thousands)		
	FY 1999	FY 2000	FY 2001
# Provide a single source of recommendations unique to DOE sites to protect against chemical and biological agents. Increase is to begin to develop, test, and evaluate prepositioning low-cost chemical and biological agent neutralization systems into the air ducts of sensitive DOE facilities. (SNLA)	500	750	900
# Develop tools to simulate DOE sites and perform risk analyses to determine the optimum security needs within current constraints. (SNLA)	250	150	150
# Capital Equipment	388	388	480
Total, Physical Security	9,318	11,128	13,275

Material Control and Accounting (MC&A)

# Develop analysis/detection capabilities for americium, neptunium, and special nuclear material contained in spent fuel, as well as extend current measurement capabilities to account for 100% of the DOE's special nuclear materials inventory. Provide technical assistance in the operation of newly developed technologies. Decrease is due to a shift in program priorities to physical security (LANL, LLNL)	5,077	4,892	4,623
# Evaluate commercial MC&A systems and technologies to determine their applicability to DOE. Decrease is due to completion of a key activity. (LANL)	460	535	360
# Develop special nuclear material standards to calibrate instruments. Increase provides a large, impure plutonium oxide nondestructive assay standard. (LANL, LLNL)	800	650	1,165
# Provide required modules to the Department's standard material control and accounting system. Decrease is a result of finishing core software. (SRS)	800	1,200	1,000
# Fund DOE's support of the National Interagency R&D Program for combating terrorism. (Funding originally included under technical assistance and maintenance to DOE sites.) (DOE-HQ)	750	750	750
# Develop DOE courses to keep personnel abreast of latest MC&A technologies and issues impacting the DOE complex. (LANL)	855	875	855
# Provide technical assistance and maintenance to DOE sites for fielded MC&A systems.	690	781	750
# Capital Equipment	364	364	364

	(dollars in thousands)		
	FY 1999	FY 2000	FY 2001
Total, Material Control and Accounting	9,796	10,047	9,867

Information Security

# Develop automated information system alarms to provide automatic, comprehensive capability to detect unauthorized activities, to evaluate these activities, and to appropriately respond. Reduction is result of reprioritization of NSS programs needs and to support the HQ guard contract under Operational Support. (Science & Tech Lab/ LLNL)	2,325	2,325	750
# Develop advanced network intrusion detection and warning sensors which are capable of sustained performance at the high bandwidth associated with the DOE cyber infrastructure. Decrease is due to increased emphasis on vulnerability fixes in physical security (LLNL, LANL, PNNL, LANL)	2,321	3,085	1,485
# Provide technical assistance on current threats to DOE information networks and determine mitigation strategies. Decrease is due to increased emphasis on vulnerability fixes in physical security (LLNL)	450	450	250
# Provide low cost experience-based training for network system administrators. (LLNL)	225	225	250
# Capital Equipment	185	185	93
Total, Information Security	5,506	6,270	2,828
Total, Technology and Systems Development	24,620	27,445	25,970

Explanation of Funding Changes from FY 2000 to FY 2001

	FY 2000 vs. FY 2001 ($ 000)
Science and Technology Development Projects	
# Major shifts within physical security include developing and implementing solutions to existing vulnerabilities at DOE sites at an increased rate (+725); increased efforts in the investigation of new delay tactics that could be deployed around the DOE complex to properly secure DOE National assets and prevent theft or diversion of special nuclear materials (+400); provide necessary advances in protective force technologies so that special response teams are properly equipped to respond to critical incidents (+800); and a shift of focus from explosives detection (-530) and advanced barriers (-490) to technical assistance to DOE sites (+1,000). Provide an increased emphasis on defenses to chemical and biological agents (+150). The shifts in MC&A are a result of increased support in the development of nondestructive assay standards (+515); and reduced efforts in developing improved measurement capabilities (-269) as a result of enhanced protective force technologies in physical security; and decreases in the evaluation of commercial MC&A systems (-175) and a material accountability system (-200) are a result of completion of core activities and minor reduction (-51) throughout MC&A training and technical assistance. Information security has been reduced (-1,604) due to required increases to the physical security program to improve safeguards and security at DOE sites through increased technical support and elimination of known vulnerabilities.	271
Technology Application	
# Reduction is a result of decreased efforts in the development of advanced information security tools	-261
Technology Support, Assistance, and Consultation Tasks	
# Reduction reflects decrease to support DOE Headquarters Protective Force contract and elimination of specific tasks and technical assistance in information security	-1,485
Total Funding Change, Technology and Systems Development	-1,475

Classification/Declassification

Mission Supporting Goals and Objectives

The Department of Energy has a unique statutory-based responsibility for the classification and declassification of nuclear weapons-related technology, known as Restricted Data. In that regard, the Classification/Declassification program's mission is to identify which of the Department's information warrants protection in the interest of national security and which information does not warrant protection. This critical program is truly the corner stone of the U.S. nuclear nonproliferation and security program since an asset cannot be protected until it is identified as requiring protection. Consistent with this mission, the Classification/Declassification program funds Management and Operating Contractors in the field and Support Service Contractors at Headquarters who provide highly technical support in a number of ways: by conducting declassification reviews and audits of documents under Statute and Executive order to identify information warranting protection from strategic adversaries, proliferants or potential proliferants and terrorists, while declassifying information critical to public discourse on the direction of the nuclear weapons program into the next century; by developing detailed classification guidance to increase the Government-wide understanding of which information requires protection in the interest of the nation's security; conducting training of personnel and appraisals of classification/declassification programs throughout Government to ensure consistent protection of the nation's most sensitive information; and by developing state-of-the-art technology to enhance the classification and declassification process, making it more efficient and effective.

Funding Schedule

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Classification/Declassification	10,213	16,667	20,884	4,217	25.3%
Total, Classification/Declassification	10,213	16,667	20,884	4,217	25.3%

Detailed Program Justification

(dollars in thousands)

	FY 1999	FY 2000	FY 2001
Classification/Declassification			
# Declassification review of documents under statutory requirements (i.e., P.L. 105-261, National Defense Authorization Act for Fiscal Year 1999, P.L. 106-65, National Defense Authorization Act for Fiscal Year 2000, the Freedom of Information Act) or Executive order requirements (i.e., Executive Order 12958, Classified National Security Information). Reviews are designed to protect sensitive nuclear weapon information from inadvertent public release throughout the Government, and to release to the public all documents not warranting protection in the interest of the nation's security.	4,980	8,740	11,250
# Classification review of newly created documents to determine which documents contain information warranting protection in the interest of the nation's security, e.g., sensitive nuclear weapon design information. Reviews are required under statutory, Executive order, litigation and Congressional requirements.	665	1,166	1,500
# Conduct training of personnel and appraisals of classification/declassification programs both internally and for other agencies. Training and appraisal programs are designed to provide consistent protection throughout the Government for sensitive nuclear weapon information, as mandated in P.L. 105-261, and 10 CFR Part 1045, Nuclear Classification and Declassification.	550	960	1,238
Maintain comprehensive classification guidance program to identify information which requires protection in the interest of the nation's security.			
# Update existing classification topics and develop new topics as programmatic needs arise.	973	1,710	2,200
# Develop guidance to implement Fundamental Classification Policy Review (FCPR) recommendations under a streamlined system, improving overall effectiveness of the classification guidance program to identify classified information. Continue effort to develop specific classification guidance implementing FCPR using page change method through mid-FY 1999. . . .	612		

(dollars in thousands)

	FY 1999	FY 2000	FY 2001
# In late FY 1999, transitioned into classification guidance streamlining, issuing prototype streamlined guide (CG-NMP-2). In FY 2000 continue classification guidance streamlining, issuing first increment of administrative/policy guidance, updating and converting CG-NMP-2 from prototype to streamlined format and initiating development of streamlined weapon design and weapon science guidance. In FY 2001, continue guidance system streamlining initiative, increasing the scope of the administrative/policy guidance, issuing weapon design and science guidance in the streamlined format, and designing the balance of system.	613	1,225	998
Development of state-of-the-art technology for document declassification to improve efficiency and effectiveness of declassification, and to protect classified information from disclosure.			
# Continue development of ultra structure knowledge-base. . . .	1,195	2,095	2,700
# Limited expansion of electronic document declassification system and testing the application of the declassification tools against a set of documents in FY 1999.	625		
# Set up test capability at one field location in FY 2000. Expand the system to multiple field sites in FY 2001, include on-site testing and implementation.		771	998
Total, Classification/Declassification	10,213	16,667	20,884

Explanation of Funding Changes from FY 2000 to FY 2001

	FY 2000 vs. FY 2001 ($ 000)
Classification/Declassification	
# Perform declassification review of documents under statutory requirements to protect sensitive information from inadvertent public release	+2,510
# Perform classification review of newly created documents to determine which documents contain information warranting protection	+334
# Train personnel and appraise classification/declassification programs both internally and for other agencies to provide consistent protection throughout the Government for sensitive nuclear weapon information	+278
# Maintain comprehensive classification guidance program by updating existing classification topics and developing new topics as programmatic needs arise while continuing guidance system streamlining initiative, increasing the scope of administrative/policy guidance	+263
# Support state-of-the-art technology for document declassification by developing an ultra structure knowledge-base and expanding electronic document declassification system to multiple field sites, including on-site testing and implementation	+832
Total Funding Change, Classification/Declassification	+4,217

Cyber Security

Mission Supporting Goals and Objectives

The goal of the Cyber Security Program is to provide consistent principles and requirements that line management can implement for the protection of classified and unclassified information used or stored on Departmental Information Systems, as required by national level laws and policies. The policies for the protection of this information will ensure that classified and unclassified information is protected consistently across the various elements of the Department in a cost-effective manner, and consistent with the protection of this information in paper form.

The program will also provide for Departmental cyber security tools and capabilities that are required by all Departmental elements. These tools and capabilities are primarily training requirements, incident response capability, and core cyber security architecture development and deployment.

FY 2001 funding will be used to ensure that the above goals will be met in a timely, efficient manner.

The Cyber Security Program has four major objective areas: Policy and Planning, Training, Operations, and Technical Development.

Policy and Planning – To provide high level consistent, risk management-based policies and implementation guidance for the protection of cyber assets.

Training – To provide consistent core training requirements for cyber security professionals, system administrators, senior management, and general users.

Operations – To provide Departmental capabilities for cyber incident response, core cyber security architecture, cyber intrusion detection and reporting, and Public Key Infrastructure (PKI) architecture.

Technical Development – To provide technical tools to eliminate cyber security vulnerabilities where commercial or Government products are not available.

Funding Schedule

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Policy and Planning		2,340	2,000	-340	-14.5%
Training		2,823	3,350	527	18.7%
Operations		7,155	23,314	16,159	225.8%
Technical Capability		1,000	1,675	675	67.5%
Subtotal, Cyber Security		13,318[a]	30,339	17,021	127.8%
Less Proposed Supplemental Request		-4,000		4,000	
Total, Cyber Security		9,318	30,339	21,021	225.6%

Detailed Program Justification

(dollars in thousands)

	FY 1999	FY 2000	FY 2001
Policy and Planning			
# Develop and maintain policies necessary to provide the framework for an integrated Cyber Security Program across the Department's varying missions and sites. Review Cyber Security Program Plans that are being developed at Departmental sites.		2,340	2,000
Training			
# Conduct Phase II training. In FY 2000, completed Phase I training for a limited number of people, began the Phase II needs analysis, and conducted baseline skills evaluation and certification for classified computer security. In FY 2001, support Phase II which will implement DOE-wide training to a broad audience. Phase II of the Cyber Security training initiative consists primarily of execution of the training courses, based on completion of the Phase II needs analysis and training plan development. The core audience for Phase II will be individuals responsible for implementing Cyber Security programs and protection measures. These include, but are not limited to managers, system administrators, Cyber Security professionals, and general users. Training will use commercial and government off-the-shelf materials where available.		2,823	3,350

[a]Appropriated to date in FY 2000, approximately $1.0 million is provided for Cyber Security in the Program Direction budget for a total amount of $10.3 million. The supplemental request proposes increasing the amount by $4.0 million.

	(dollars in thousands)		
	FY 1999	FY 2000	FY 2001
Operations			
Provide for continued cyber security incident response capabilities, DOE-wide implementation of baseline cyber security architecture, and enhanced Public Key Infrastructure (PKI) deployment.			
# Maintenance of incident response capability (Computer Incident Advisory Capability (CIAC) at LLNL)). Provide support for a total of 15 contractor FTEs to provide cyber security incident response, analysis of cyber intrusions and attempted intrusions, and warning capability for the Department. FY 2000 provided partial year funding for support, FY 2001 supports contractor level for the entire year.		3,337	5,000
# Cyber Security Core Architecture engineering and deployment – FY 2000 supported design of the baseline cyber security capability. In FY 2001, implement baseline cyber security architecture at 12 sites.		2,114	15,696
# Classified Systems Support – Provide funding for classified system support including IV and V for accreditation of classified systems. In FY 2001, funding provides for a classified DOE information server and accompanying technical support.		300	618
# PKI Initiative – Provide funding to operate and expand inter-site PKI capability for the protection of unclassified data in transit, as well as limited capability for protection of unclassified data in storage. Funding also provides for Departmental infrastructure to support token or biometric authentication and allows for coordination and unification of previously independent PKI efforts.		1,404	2,000
Total, Operations		7,155	23,314

(dollars in thousands)

	FY 1999	FY 2000	FY 2001
Technical Capability			
# Provides funding for technical support and minimal R&D efforts. Additional funds in FY 2001 will support the establishment of a limited testing capability for commercial off-the-shelf (COTS) cyber security products prior to being deployed in the Department. There is a continuous need to evaluate and potentially modify COTS cyber security products to ensure that the application of these products does not significantly interfere with primary organizational or computer missions, and to identify weaknesses in COTS products that must be mitigated to ensure a consistent, comprehensive cyber security implementation.		1,000	1,675
Subtotal, Cyber Security		13,318	30,339
Less Proposed Supplemental Request		-4,000	
Total, Cyber Security		9,318	30,339

Explanation of Funding Changes from FY 2000 to FY 2001

	FY 2000 vs. FY 2001 ($ 000)
Cyber Security	
Policy and Planning	
# Maintain policies for an integrated Cyber Security Program including review of cyber security program plans being developed at Departmental sites	-340
Training	
# Support Phase II of cyber security training which implements enterprise-wide training to individuals primarily responsible for implementing cyber security programs and protection measures	+527
Operations	
# Provide full year funding for M&O contractor support at LLNL for CIAC	+1,663
# Implement baseline cyber security architecture at 12 sites	+13,582
# Provide a classified DOE information server and accompanying technical support	+318
# Provide ability to operate and expand inter-site PKI capability for protection of unclassified data in transit and the infrastructure to support token or biometric authentication, allowing coordination and unification of previously independent PKI efforts	+596
Technical Capability	
# Establishment of limited testing capability for commercial off-the-shelf cyber security products prior to being deployed in the Department	+675
Subtotal Funding Change, Cyber Security	+17,021
Adjustment for Proposed FY 2000 Supplemental Request	+4,000
Total Funding Change, Cyber Security	+21,021

Capital Operating Expenses and Construction Summary

Capital Operating Expenses

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Capital Equipment	5,496	1,496	1,496	0	0%
Total, Capital Equipment	5,496	1,496	1,496	0	0%

Security Investigations

Program Mission

The Security Investigations Program funds background investigations for all DOE Federal staff and all Headquarters contractors, who, in the performance of their official duties, require access authorizations for Restricted Data, National Security Information, or special nuclear material. User program organizations will fund field office requests for background investigations for contractors and non-Federal personnel who are not included in the Security Investigations Program budget.

Program Goal

Support the common defense and security of the United States by ensuring that only appropriate personnel are authorized access to classified information, special nuclear material, or occupy sensitive positions.

Program Objectives

- Ensure the timely and efficient processing and adjudication of initial access authorization and reinvestigations.
- Ensure that the types and numbers of access authorizations are consistent with DOE mission changes, taking into consideration heightened security requirements.
- Ensure that the quality of an investigative product is sufficient for DOE security needs.
- Support development and implementation of an electronic network among DOE field offices, DOE contractors, the Office of Personnel Management (OPM) and other Federal agencies to reduce the overall access authorization processing time.

Performance Measures

- Conduct approximately 16,270 personnel security investigations and reinvestigations for the total DOE-wide program.
- Align the numbers and levels of access authorizations with identified heightened statutory security requirements.

Significant Accomplishments and Program Shifts

- In FY 1999, the user program organizations provided additional funding, as outlined in the Notification Letter to Congress, which helped eliminate the increasing reinvestigation backlog.

- In order to ensure that the number of security clearances is consistent with mission requirements, the number of "Q" access authorizations may begin to increase in FY 2000 due to heightened security awareness.

- In FY 1999 and FY 2000, funding for the Security Investigations program was appropriated in the Nonproliferation and National Security budget requests. As a result of the DOE-wide security reform announced on May 11, 1999, the Security Investigations program was transferred to the new Office of Security and Emergency Operations. Beginning with FY 2001, funding for this program will be budgeted for in the new Office of Security and Emergency Operations budget request.

- As a result of the Defense Authorization Act for FY 2000 (S.1059, Section 3144) there has been a change in policy requiring certain personnel in positions that are of such a critical nature that any compromise could gravely impact U.S. national security to have background investigations conducted by the FBI. The FBI product is almost double the cost of the OPM background investigation product. People in less sensitive positions will continue to have their investigations performed by the Office of Personnel Management.

Funding Profile

(dollars in thousands)

	FY 1999 Current Appropriation	FY 2000 Original Appropriation	FY 2000 Adjustments	FY 2000 Current Appropriation	FY 2001 Request
Security Investigations					
Security Investigations	38,145	33,000	-336[a]	32,664	33,000
Off-sets from Program Organizations	-28,145[b]	-20,000		-20,000	-20,000
Subtotal, Security Investigations	10,000	13,000	-336[a]	12,664	13,000
Use of Prior-Year Balances	-630[c]				
Total, Security Investigations	9,370	13,000	-336[a]	12,664	13,000

Public Law Authorization:
Public Law 83-703, "Atomic Energy Act of 1954"

[a]Reflects Government-wide rescission in the Consolidated Appropriations Act for FY 2000 assigned to this program.

[b]While the Congressional Budget identified an offset of $20M, the Controller's Office subsequently notified the Congress that the Department would allocate up to $35M from Program Organizations to fund additional security investigation requirements.

[c]Reflects EWD reduction for use of prior-year uncosted balances ($630,000) assigned to this program.

Funding by Site

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Albuquerque Operations Office	13,767	8,779	8,371	-408	-4.6%
Chicago Operations Office	409	246	305	+59	+24.0%
Idaho Operations Office	508	476	499	+23	+4.8%
Nevada Operations Office	641	564	639	+75	+13.3%
Oak Ridge Operations Office					
Oak Ridge Operations Office	4,758	2,993	3,172	+179	+6.0%
Oak Ridge Institute of Science & Education.	300	150	150	0	0%
Total, Oak Ridge Operations Office	5,058	3,143	3,322	+179	+5.7%
Pittsburgh Naval Reactors Office	1,850	1,234	1,145	-89	-7.2%
Richland Operations Office	1,206	725	777	+52	+7.2%
Oakland Operations Office	2,902	2,885	2,885	0	0%
Savannah River Operations Office	1,954	2,387	2,496	+109	+4.6%
Schenectady Naval Reactors Office	550	461	461	0	0%
Washington Headquarters	9,300	11,764	12,100	+336	+2.9%
Subtotal, Security Investigations	38,145	32,664	33,000	+336	+1.0%
Off-sets from Program Organizations	-28,145[d]	-20,000	-20,000	0	0%
Use of Prior Year Balances	-630				
Total, Security Investigations	9,370[e]	12,664[f]	13,000	+336	+2.7%

[d]While the Congressional Budget identified an offset of $20M, the Controller's Office subsequently notified the Congress that the Department would allocate up to $35M from Program Organizations to fund additional security investigation requirements.

[e]Reflects EWD reduction for use of prior-year uncosted balances ($630,000) assigned to this program.

[f]Reflects Government-wide rescission in the Consolidated Appropriations Act for FY 2000 ($336,000) assigned to this program.

Site Description

Operations Offices

For each of the DOE Operations Offices listed in "Funding by Site," one or more of four program organizations (Defense Programs, Environmental Management, Science, and Nuclear Energy) provide funding to the Personnel Security Offices to pay for background investigations conducted by the Federal Bureau of Investigation (FBI) and the Office of Personnel Management (OPM) for contractors and non-federal personnel who are not included in the Security Investigations Program budget funded out of Headquarters. Total Program Organization offsets are limited to $20 Million. Background investigations are required for personnel who, in the performance of their official duties, require access to classified information or special nuclear material. The investigation is one of the tools used by DOE security personnel to determine if an individual will receive a security clearance.

Washington Headquarters

The Security Investigations Program provides funding for background investigations conducted by the FBI and OPM for DOE-wide Federal staff and Headquarters contractors. This program also supports programs under Related Security Investigations Activities required to assure a viable personnel security function. This includes enhancements to the Electronic Transfer Program and DOE Integrated Safeguards and Security (DISS) personnel security databases to support additional functionality and security features.

Security Investigations

Mission Supporting Goals and Objectives

The Security Investigations budget funds background investigations for DOE Federal personnel and Headquarters contractors who, in the performance of their official duties, require access authorizations for Restricted Data, National Security Information, or special nuclear material. User program organizations will fund field office requests for background investigations for contractor and non-Federal personnel who are not included in the Security Investigations budget. Security Investigations are required in order to be in compliance with Section 145 of the Atomic Energy Act of 1954, as amended; Title 10, Code of Federal Regulations, Part 710; and Executive Order 12968, which mandate that access authorizations (security clearances) are required for access to classified information or special nuclear material. The Department primarily utilizes the services of the Office of Personnel Management (OPM) to conduct security investigations which serve as the basis for these access authorizations. FBI investigations are now required for individuals in positions that are of such a critical nature that any compromise could gravely impact U.S. national security. The cost of security investigations depends on the type and level of investigation needed.

The Budget Request includes funds for all departmental clearances. However, due to accelerated program requirements, cleanup efforts, and security requirements at the DOE sites, additional clearances for DOE contractors may be required. Therefore, the Department may seek to increase the limit on Program Organization offsets, which is currently limited to $20 million, in FY 2000 and FY 2001. For FY 1999, the Department increased this limit to $35 million.

Funding Schedule

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Federal Bureau of Investigation Background Investigations	49	2,026	2,990	+964	+47.6%
Office of Personnel Management					
Initial Background Investigations	12,777	9,926	8,146	-1,780	-17.9%
Reinvestigations	21,556	16,455	16,587	+132	+0.8%
National Agency Checks	423	447	467	+20	+4.5%
Personnel Security Review	0	0	1,000	+1,000	+100%
Total, Office of Personnel Management	34,756	26,828	26,200	-628	-2.3%
Related Security Investigations Activities	3,340	3,810	3,810	0	0.0%
Subtotal, Security Investigations	37,515	32,664	33,000	+336	+1.0%
Use of Prior Year Balances	-630				
Off-sets from Program Organizations	-28,145[a]	-20,000	-20,000	0	0.0%
Total, Security Investigations	9,370[b]	12,664[c]	13,000	+336	+2.7%

Case Projections

Category	FY 1999	FY 2000	FY 2001
Federal Bureau of Investigation Background Investigations	9	356	530
Office of Personnel Management			
Initial Background Investigations	3,707	3,202	2,628
Reinvestigations	13,078	10,300	9,070
National Agency Checks	3,674	3,889	4,042
Subtotal, Office of Personnel Management Investigations	20,459	17,391	15,740
Total, Security Investigations	20,468[d]	17,747	16,270

[a]While the Congressional Budget identified an offset of $20M, the Controller's Office subsequently notified the Congress that the Department would allocate up to $35M from Program Organizations to fund additional security investigation requirements.

[b]Reflects EWD reduction for use of prior-year uncosted balances ($630,000) assigned to this program.

[c]Reflects Government-wide rescission in the Consolidated Appropriations Act for FY 2000 ($336,000) assigned to this program.

[d]Due to Program Organizations allocating additional funds for security investigations, the number of cases increased from what was originally budgeted for in FY 1999.

Detailed Program Justification

	(dollars in thousands)		
	FY 1999	FY 2000	FY 2001
Federal Bureau of Investigation (FBI)			
# Conduct up to 530 initial FBI background investigations and reimburse the FBI for fingerprint cards and name checks. This represents a change in policy requiring certain personnel in positions that are of such a critical nature that any compromise could gravely impact U.S. national security, to have FBI background investigations, rather than OPM background investigations. Additional funds from Program Organizations would be required to prevent the possibility of a substantial backlog	49	2,026	2,990
Office of Personnel Management			
# Anticipate 2,628 OPM initial (Single Scope Background) investigations in FY 2001. Decrease is necessary to increase FBI and reinvestigation funding. Additional offsets from Program Organizations would be required in order to meet program requirements due to developing programs, accelerated cleanup efforts, and an increase in the number of "L" initial upgrades from National Agency Checks to full-field background investigations due to heightened security requirements. Plan to support 3,202 cases in FY 2000. Funded 3,707 cases in FY 1999 due to Program Organizations being able to contribute their funds to this program	12,777	9,926	8,146
# Perform 9,070 OPM periodic reinvestigations (for Single Scope Background Investigations) in FY 2001. Additional offsets would be required from Program Organizations in order to prevent the possibility of a substantial backlog. Project 10,300 cases in FY 2000. Funded 13,078 cases in FY 1999 due to Program Organizations being able to contribute their funds to this program	21,556	16,455	16,587
# Conduct 4,042 National Agency Checks (NAC's) in FY 2001. Plan to support 3,865 NAC's in FY 2000 and 3,674 NAC's in FY 1999.	423	447	467

	(dollars in thousands)		
	FY 1999	FY 2000	FY 2001
# Conduct a personnel security review for certain selected positions using an automatic expansion of the investigations where derogatory information is discovered. Also, evaluate the use of OPM rather than FBI for certain sensitive positions, to determine the best practice available for "elevated" clearances.	0	0	1,000
Total, Office of Personnel Management	34,756	26,828	26,200
Related Security Investigations Activities			
# Continue operation and maintenance of the Electronic Transfer Program throughout DOE	2,430	2,900	2,900
# Continue to support Accelerated Access Authorization Program (AAAP)	600	600	600
# Provide support for miscellaneous costs involved in maintaining a viable personnel security program	310	310	310
Total, Related Security Investigations Activities	2,710	3,810	3,810
Subtotal, Security Investigations	37,515	32,664	33,000
Use of Prior Year Balances	-630		
Off-sets from Program Organizations	-28,145[a]	-20,000	-20,000
Total, Security Investigations	9,370[b]	12,664[c]	13,000

[a]While the Congressional Budget identified an offset of $20M, the Controller's Office subsequently notified the Congress that the Department would allocate up to $35M from Program Organizations to fund additional security investigation requirements.

[b]Reflects EWD reduction for use of prior-year uncosted balances ($630,000) assigned to this program.

[c]Reflects Government-wide rescission in the Consolidated Appropriations Act for FY 2000 ($336,000) assigned to this program.

Explanation of Funding Changes from FY 2000 to FY 2001

	FY 2001 vs. FY 2000 ($000)
Federal Bureau of Investigation (FBI)	
# FBI funding level reflects increase due to change in policy requiring certain individuals in critical positions to have this type of investigation	+964
Office of Personnel Management	
# Initial Office of Personnel Management (OPM) background investigation estimates are based on specific site and contractor needs. Decrease is necessary to reduce backlog of reinvestigations at this level of funding and increase funding for FBI	-1,780
# OPM reinvestigation activities have been increased in order to limit the backlog. A $20 million off-set from program organizations would be inadequate and additional funds are required to prevent a backlog	+132
# National Agency Checks are now budgeted for initial "L" clearances and reinvestigations. Changes in funding reflect specific site and contractor needs	+20
# OPM investigations for certain selected positions will be conducted using an automatic expansion of the investigation by OPM where derogatory information is discovered. This will lesson the steps involved in the resolution of cases, at an additional cost per case. Another review will be conducted regarding the use of the FBI rather than OPM for certain sensitive positions, as mandated by Congress, in determining the best practices available for “elevated” clearances	+1,000
Total, Security Investigations	+336

Security and Emergency Operations Program Direction

Mission Supporting Goals and Objectives

The Security and Emergency Operations (SO) program direction budget provides for all Federal personnel required at DOE Headquarters, and two field offices to carry out the program's mission in a cost effective and efficient manner. The budget request for SO reflects the reorganization into this office of the Emergency Response function, formerly budgeted for in Defense Programs, the Chief Information Officer function, formerly budgeted in the Departmental Administration account, and the Office of Security Affairs, Emergency Management, and portions of Resource Management, formerly budgeted in the Nonproliferation and National Security account.

Program Goals

Provides the salaries and benefits, travel, support service contracts, and other related expenses associated with the overall management, direction, and administration of the following programs:

Nuclear Safeguards and Security
Nuclear and National Security Information (Formerly the Office of Declassification)
Emergency Management
Chief Information Officer (CIO)
Plutonium, Uranium, and Special Material Inventory
Foreign Visits and Assignments
Critical Infrastructure Program

Program Objectives

- To provide Salaries and Benefits for SO Federal employees, including overtime, awards, lump sum leave payments, transit subsidies, contributions to employee benefits, and associated escalation.
- To provide travel funds that are required to carry out the program mission while away from official duty stations (per diem allowances as well as local travel) and to fund the Executive Protection Security Program travel which was realigned in FY 2000 from the Office of the Secretary of Energy to the Office of Security and Emergency Management. Travel is an essential part of staff duties in order to conduct hands-on operations both domestically and internationally, participate in highly technical agency and interagency committees, and to ensure appropriate Government representation in policy meetings.

To provide Support Services contracts funding for multiple program areas:

- provide support services contract funding for technical and analytical support to the initiatives of the Chief Information Officer based on the Clinger-Cohen Act, operational and infrastructure requirements.
- provide technical, analytical, administrative, and operational support in multiple program areas of safeguards and security; critical infrastructure; and emergency management. The daily operation and associated technical direction of the contracts remain with Federal program managers in each organization.

To provide funding for Other Related Expenses, including the working capital fund (space, utilities, general printing, graphics, copying, supplies, telephones, etc.), general office automation support, operation and maintenance of equipment, and other miscellaneous services.

Performance Measures

The principal objective of Program Direction is to provide the appropriate level of funding in the four categories supported in this budget: Federal salaries and benefits, travel, support services, and other related expenses.

The ultimate measure for success in the Program Direction subprogram is whether the Federal personnel in the various programs in Security and Emergency Operations have their salaries and benefits provided, travel funding is adequate to allow the appropriate amount of onsite supervision by the Federal staff, and the level of support services provided to the Federal staff is adequate to allow SO to perform its programmatic goals and objectives.

The performance measure for the support of the business line activities funded under the Working Capital Fund (WCF) is to control costs associated with these business lines where possible and to adequately fund these activities through the budget process. SO regularly monitors all business lines funded in the WCF and has reduced, to the extent possible, utilization of services provided through this fund. Further per capita reductions, in keeping with good business practices, in utilization of the services provided through this fund is a performance measure SO sets for itself in this account.

The performance measures for the Chief Information Officer function, whose budget request was formally imbedded in the Departmental Administration budget request are:

Develop annual operational Information Technology Plan linked to the budget process.

Measure organizational satisfaction with the timeliness and quality of the Web-based, paperless policy creation and distribution system.

Eliminate shadow human resource systems and duplicative legacy systems.

Improve availability and increase reliability of the corporate network.

Reduce policy approval time by 80%.

Funding Schedule

(dollars in thousands, whole FTEs)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Chicago					
Salaries and Benefits	3,894	4,069	4,408	+339	+8.3%
Travel	150	153	153	0	0.0%
Support Services	0	0	0	0	0.0%
Other Related Expenses	1,593	1,627	1,444	-183	-11.2%
Total, Chicago	5,637	5,849	6,005	+156	+2.7%
Full Time Equivalents	56	56	58	+2	+3.6%
Nevada					
Salaries and Benefits	621	450	168	-282	-62.7%
Travel	46	46	29	-17	-37.0%
Support Services	400	379	0	-379	-100.0%
Other Related Expenses	4	4	6	+2	+50.0%
Total, Nevada	1,071	879	203	-676	-76.9%
Full Time Equivalents	5	5	2	-3	-60.0%
Headquarters					
Salaries and Benefits	33,616	37,022	42,769	+5,747	+15.5%
Travel	1,210	1,872	1,913	+41	+2.2%
Support Services					
Support Services - Other	7,505	7,979	7,949	-30	-0.4%
Support Services - CIO	13,522	10,312	10,290	-22	-0.2%
Support Services - CIP	0	750	900	+150	+20.0%
Total, Support Services	21,027	19,041	19,139	+98	+0.5%
Other Related Expenses	16,799	17,134	19,338	+2,204	+12.9%
Total, Headquarters	72,652	75,069	83,159	+8,090	+10.8%
Full Time Equivalents	324	340	380	+40	+11.8%

	(dollars in thousands, whole FTEs)				
	FY 1999	FY 2000	FY 2001	$ Change	% Change
Total Security and Emergency Operations					
Salaries and Benefits	38,131	41,541	47,345	+5,804	+14.0%
Travel	1,406	2,071	2,095	+24	+1.2%
Support Services					
Support Services - Other	7,905	8,358	7,949	-409	-4.9%
Support Services - CIO	13,522	10,312	10,290	-22	-0.2%
Support Services - CIP	0	750	900	+150	+20.0%
Total, Support Services	21,427	19,420	19,139	-281	-1.4%
Other Related Expenses	18,396	18,765	20,788	+2,023	+10.8%
Sub-Total, Program Direction	79,360	81,797[a/]	89,367	+7,570	+9.3%
Use of Proposed Supplemental		-4,000		+4,000	
Use of Prior Year Balances	-180				
Total Program Direction	79,180	77,797	89,367	11,570	14.9%
Full Time Equivalents	385	401	440	+39	+9.7%

[a] Includes $4.0 million FY 2000 proposed supplemental. This supplemental provides for Headquarters: $1.8 million to sustain current staffing levels, $1.7 million to support an increase of 16 Federal FTEs, 0.1 million for travel cost and 0.4 million in other related expenses.

Detailed Program Justification

(dollars in thousands)

	FY 1999	FY 2000	FY 2001
Salaries and Benefits	38,131	41,541	47,345

Headquarters federal staffing is driven by specific functional responsibilities as well as management and direction requirements.

- SO staff serves as the headquarters operational element for activities such as emergency management; security, including safeguards and security, critical infrastructure activities, enhanced foreign visits and assignments activities, and plutonium, uranium, and special material inventory activities; and declassification and classification operations, and provides staff for Office of the Director and Resource Management.
- Staff develops Department-wide policy and plans for national security programs such as safeguards and security, nuclear and national security information, the Chief Information Officer, and emergency management. SO is directly responsible for management of the New Brunswick National Laboratory, the Nonproliferation and National Security Institute in Albuquerque, New Mexico, and the HAZMAT Spills Test Facility at the Nevada Test Site.
- Staff of the Chief Information Officer function develop and issue policy, procedures, and guidance on the management of information and information technology across the Department; and establish, implement, and maintain a comprehensive cyber/computer security program to protect the Department's classified and unclassified information and information technology assets.

(dollars in thousands)

	FY 1999	FY 2000	FY 2001
# Staff in the Foreign Visits and Assignments function develop and promulgate policy and guidance and perform in depth program oversight for all foreign visits and assignments to DOE and DOE contractor facilities nation-wide (including DOE Headquarters and the National laboratories) and for foreign national contact with DOE and DOE programmatic and technical persons. The Office acts as a central accounting center to track and analyze the details of all foreign visits and assignments to all DOE and DOE contractor facilities to ensure that these are conducted in a secure manner.			
# Staff in the Office of Plutonium, Uranium, and Special Materials Inventory are responsible for the accurate and reliable tracking of strategic nuclear materials and analysis of nuclear material inventory data for purposes of identifying accountability-related issues.			
Travel	1,406	2,071	2,095
# Includes domestic and foreign trips necessary to conduct security, emergency operations, and the Chief Information Officer's activities.			
# Domestic travel includes national security assistance and interface with field offices, laboratories and local governments.			
# FY 2000 and FY 2001 provides travel for the Executive Protection Security personnel. This activity has been realigned from the Office of the Secretary of Energy to the Office of Security and Emergency Operations.			
Support Services	21,427	19,420	19,139
# Provides an invaluable resource of highly specialized and analytical expertise required to meet critical security and emergency operations issues.			
# Provides technical and analytical expertise as well as management support essential to carry-out the safeguards and security program.			

(dollars in thousands)

	FY 1999	FY 2000	FY 2001
# Provides a proactive program that interfaces with the private sector, other government agencies, and the executive branch in establishing mutual support arrangements in the furtherance of the DOE Critical Infrastructure Protection (CIP) Program.			
# Provides technical and analytical support to initiatives of the Chief Information Officer (CIO) based on the Clinger-Cohen Act, operational and infrastructure requirements.			
Other Related Expenses	18,396	18,765	20,788
# Includes Headquarters space, utilities, general printing, graphics, copying, supplies, telephones, general automation support, payroll processing, postage, and other miscellaneous expenses associated with office operations.			
# Similar support is provided to the Federally staffed New Brunswick Laboratory.			
# SO funding for the Working Capital Fund is included in this subprogram.			
Use of Prior Year Balances	(180)		
Total, Program Direction	79,180	86,792[a/]	89,367

[a] Includes $4.0 million FY 2000 proposed supplemental.

Explanation of Funding Changes

from FY 2000 to FY 2001

	FY 2001 vs. FY 2000 ($000)
Salaries and Benefits	
# Salaries and Benefits increased to fund additional FTEs ((+4,474,000)39 FTEs) and provide escalation for Federal Salaries and Benefits (+1,329,000).	+5,804
Travel	
# Travel minor adjustment.	+24
Support Services	
# Support Services - Other reduction to ongoing contracts	-409
# Support Services - Critical Infrastructure increased technical support.	+150
# Support Services - CIO decreased slightly.	-22
Other Related Expenses	
# Other Related Expenses increased to provide escalation and associated costs of additional FTEs and current staff.	+2,023
Use of Proposed Supplemental	+4,000
Total Funding Changes, Program Direction	+11,570

Support Services

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Technical Support Services					
Other Support Services	6,719	7,104	6,907	-197	-2.8%
Chief Information Officer	10,867	8,765	8,762	-3	-0.0%
Critical Infrastructure Program	0	637	765	+128	+20.1%
Total Technical Support Services	17,586	16,506	16,434	-72	-0.4%
Management Support Services					
Other Support Services	1,186	1,254	1,042	-212	-16.9%
Chief Information Officer	2,655	1,547	1,528	-19	-1.2%
Critical Infrastructure Program	0	113	135	+22	+19.5%
Total, Management Support Services	3,841	2,914	2,705	-209	-7.2%
Total Support Services	21,427	19,420	19,139	-281	-1.4%

Other Related Expenses

(dollars in thousands)

	FY 1999	FY 2000	FY 2001	$ Change	% Change
Working Capital Fund	9,127	9,583	9,775	+192	+2.0%
Training	423	948	989	+41	+4.3%
Other[a/]	8,846	8,234	10,024	+1,790	+21.7%
Total, Other Related Expenses	18,396	18,765	20,788	+2,023	+10.8%

[a]Other includes equipment and the operation and maintenance of equipment.